Elizabeth I. Peele. Forming Your Terrorist Network: ISIS, Twitter, and the Terrorist Propaganda Campaign. A Master's Paper for the M.S. in IS degree. April, 2015. 77 pages. Advisor: Mohammad Hossein Jarrahi

Since the founding of the Caliphate in June 2014, the Islamic State of Iraq and Syria has gained worldwide media attention for its campaign of violence across Iraq and Syria. Social media, particularly Twitter, has become a main aspect of ISIS's media campaign. It has been used to spread propagandistic images and videos of ISIS into the Twittersphere. This propaganda is important to ISIS because it spreads their message far past its occupied borders and helps to gain support from a wider audience. Using social media analysis and Twitter's own APIs, this research focused on ISIS's Twitter propaganda campaign and sought to discover the underlying network structure. The resulting network structure – scale-free – is then analyzed to see how it affects ISIS's dissemination of propaganda on Twitter. Ultimately, this research hopes to start a conversation on how network structure can be used to stop terrorist organizations from spreading their message online.

Headings:

Network analysis -- communication

Social network analysis

Social media – research

Terrorism – Islamic State

FORMING YOUR TERRORIST NETWORK: ISIS, TWITTER, AND THE TERRORIST PROPAGANDA CAMPAIGN

by
Elizabeth I. Peele

A Master's paper submitted to the faculty
of the School of Information and Library Science
of the University of North Carolina at Chapel Hill
in partial fulfillment of the requirements
for the degree of Master of Science in
Information Science.

Chapel Hill, North Carolina

April 2015

Approved by

_____

Mohammad Hossein Jarrahi

Table of Contents

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION

Social media has quickly become an information platform that is used by millions around the world (Kaplan & Haenlein, 2010). The posts, tweets, images, and videos posted to these sites show a bit of the world from many varied perspectives (Shirky, 2011). But, as these different information systems have risen to the forefront, they are also being used not to just show the daily happenings in a normal life but also to inform and gain support for various campaigns. These campaigns may run from the political, such as the 2014 US Congressional campaigns (Druckman, Kifer, & Parkin, 2014) to pop culture, such as who will win on The Voice or American Idol (Signorini, 2014). These larger campaigns, however, are not all as innocuous as who is the "best" singer in the competition. Indeed, some of these campaigns focus on propagandizing for a cause that has been designated as a terrorist threat from multiple nations and multi-national organizations. The most sophisticated of these "global jihadi" social media campaigns comes from the Islamic State of Iraq and Syria (ISIS) (al-Tamimi, 2014, p.8). ISIS has a developed and masterful social media campaign designed to attract the greatest amount of attention from the greatest amount of people in the hopes of turning some of these people towards their cause and jihadi ideology.

While ISIS is not the only terrorist organization using social media, they have shown themselves to – so far – be the best at manipulating social media's resources to serve their cause and the best coordinated presence on social media (Glint, 2014). The social media platform they are currently the best at manipulating and using is Twitter

(Providence Research, 2014). Through tweeting, ISIS disseminates their "brand image" to the world and creates networks where ISIS militants and supporters can come together. These connected networks allow militants, supporters, sympathizers, and administrators to spread information to a large, public audience.

Research and Motivation

The motivation for this research paper centers around understanding the networks ISIS forms on Twitter. These Twitter networks are the points of information distribution for ISIS's Twitter campaign; from these points comes most of the data. By moving from the overall Twitter base, to recognizing these center points, an overall greater knowledge about these network structures can be found. The rationale behind this study is that by completing it and gaining the knowledge it provides, a solution can begin to form on how to combat ISIS on Twitter. This thesis seeks to understand the flow of information and the social network relationships by looking at how ISIS English-language users are propagandizing through the social platform of Twitter.

Understanding the overall network structure ISIS uses on Twitter is important because this network is being used to gain supporters for a malicious cause, and while authorities believe that suspending accounts is helping to slow ISIS propaganda on Twitter, they have not figured out a way to more effectively slow down these networks (Berger, 2015). While ISIS accounts on Twitter may be growing more slowly than in the past (Berger, 2015), they are still using other social media sites such as Diaspora (Stone, 2014), and understanding their social network structure for one major social media outlet could give a better understanding to how they will grow their propaganda campaign on a new social media outlet. As ISIS continues to post videos, photos, and messages about

executions, hostages, magazines, and other forms of propaganda, it is important to understand the overall network of this dissemination in order to best know how to dismantle such a terrorist network.

While ISIS uses Twitter for all the reasons mentioned above, one of its big purposes – and the main focus of this study – is propaganda. Propaganda is a popular topic of study, especially in communication studies, and has many definitions. For this research, propaganda will be used in accordance with the following definition:

> *Propaganda* is a deliberate and systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist. (Jowett & O'Donnell, 2006, p. 269).

According to this definition, many things that ISIS tweets can be considered propaganda because it is an overall campaign meant to manipulate perceptions and cognitions. This research will focus more on propaganda as a reaction to critical incidents rather than more mundane details about life mainly because reactional data is easier to track and gather.

This reactional data will help to show the configuration of the ISIS's overall Twitter network. Journalists, analysts, and government-sponsored agencies have written about ISIS's sophisticated Twitter campaigns (Providence Research, 2015). Much of this sophistication, and the outreach it allows, arises from both gaming the social media system and, perhaps more importantly, from the overall structure of the network. The network balances between centralized and decentralized in order to spread its propaganda campaign as far as possible. This fragmentedness (Walker, 2015) results in there being the centralized, professional media campaign that is disseminated by the higher-up authorities in ISIS, and then the decentralized, "independent actors" (Kingsley, 2014),

who seem to spread this information to a larger population of social media users. It is this balanced network that has helped to form the "sophisticated online propaganda machine" (Zayadin, 2015) currently influencing the ISIS battlefields and the world's home front. The configuration of the network structure is important in understanding how and why this balancing act between centralized and decentralized has been so effective.

Research Questions

This research paper will seek to find answers to the questions of:

1. How does the configuration of ISIS's Twitter network affect the dissemination of its propaganda?
    1.1 Does ISIS's dissemination of propaganda information on Twitter result in more than one central actor responsible for the dissemination of information on Twitter?
    1.2 What is the role of the central actor responsible for dissemination of information?
    1.3 How do other actors carry forward the propaganda articulated by the central actor?

These questions seek to unearth how ISIS's disseminates their propaganda on Twitter, and what network structure this dissemination takes. Understanding the network structure is important for discovering how users get their information, and from a government standpoint, how this spread of information could be attacked and shut down. ISIS may be the first terrorist group to use Twitter as effectively as they have, but more terrorist groups will learn from them, and will take these tactics as their own. Learning now how terrorists disseminate propaganda information can provide help in the future for fighting against cyber propaganda from extremist groups

RESEARCH BACKGROUND AND LITERATURE REVIEW

Brief History of Social Media

Within the last ten-to-fifteen years, the use of social media on the Internet has exploded. As of July 2014, Facebook reported 1.32 billion monthly active users with users spending an average of 40 minutes each day browsing the social networking site (Brustein, 2014). YouTube reports statistics of 1 billion unique users each month with 80% of its traffic coming from outside the United States. These users then reportedly watch a collective 6 billion hours of video each month (YouTube, 2014). Twitter, one of the newer social media technologies, already attracts 284 million monthly active users who tweet more than 500 million tweets a day (Twitter, 2014). Of these user accounts, 77% of them are outside the United States. These are remarkable statistics for technologies that have only been around for ten-to-fifteen years at the most. And while social media is used for all types of activities, from the mundane—tweeting about what you are wearing or where you are going—to the remarkable—finding a biological family member or thanking a stranger for an act of kindness—the uses of social media and its impact on society are still being explored.

Terrorism, propaganda, and use of social media

One of the more controversial usages of social media is its use by terrorists, terrorist organizations, and individuals claiming to wage 'jihad.' Terrorist groups have long used the Internet as a platform for disseminating information, planning, recruiting, and financing (Weimann, 2014). Gabriel Weimann, a noted expert on terrorism and the

Internet, provides brief history of how far terrorist organizations have come since 1998, when only about 15 designated Foreign Terrorist Organizations had a web presence (2004). By 2000, most organizations had a presence on the web and official ways to communicate with followers and supporters. Most of this online communication was done in the early years by top-down websites and then later, on interactive forums (Zelin, 2013). The top-down websites held a "complete monopoly" (Zelin, p. 4, 2013) over the content of the website. The jihadi organizations would post official material, press releases, and videos here, and this material would then be filtered down through the users. It was not interactive, nor did it allow common, individual, users to upload their own materials. Instead, all materials were approved and displayed based on the site administrators who were normally hand-chosen by the jihadi organization to approve such content or directed to add materials immediately for distribution.

As the Internet gained traction, and more and more terrorist organizations moved their materials to the web, interactive forums and emailing groups began to pop up. These forums and groups existed (and still exist) not just on the Dark Net but also in more common places like Google and Yahoo communities (Denning, 2009). These forums and emailing groups provide a way for jihadists, want-to-be-jihadists, and jihadist supporters to interact with each other without identifying who they are. A posting on a jihadist forum actually explains the process of setting up a fake Google or Yahoo account in order to start one of these groups (Weimann, 2011). These forums and groups are intriguing because they show the evolution from top-down mandated content to a more interactive organization. The users of the forums and the groups themselves can post content and discuss information (Zelin, 2013). While this information can then be

deleted and the user possibly banned, it does allow for more dialogue amongst the general users. However, these forums and groups are still authenticated and only allow people who are already members of the forum or who have been invited to the group to participate in the discussion.

This authentication of data and users rapidly changes with the introduction of social media platforms. With the introduction of Youtube in 2005 (Youtube, 2014), Facebook in 2006 (Facebook, 2014), and Twitter in 2006 (Twitter, 2014), the ability to network and disseminate information online became easier than ever.[i] The leader of Al-Qaeda after Osama bin-Laden's death, Ayman al-Zawahiri, acknowledged the powerful use of media by stating that "[m]ore than half [of what the United States considers terrorism] is taking place on the battlefield of the media, [for] we are in a media battle for the hearts and minds [of Muslims]" (al-Zawahiri, 2006 as cited by Archetti, 2012). Not only did this expansion into the media and social media realms allow for easier access to jihadists in various parts of the world but it also made it easier to connect with non-jihadists who could be swayed to support the movement (Seib & Janbek, 2010). Along with this ease of access, it also gave the individuals of these organizations more power because they could post their own 'original' content instead of just re-issuing what the administrators of a site posted. For ISIS, this means that their fighters on the ground have just as much sway over the hearts and minds of possible supporters on Twitter as top officials do (Hall, 2015). Their posts about daily life or about ideology are just as strong of propaganda as any authenticated information (Hall, 2015). No longer is the communication network solely comprised of top-down websites or authenticated forums;

instead, anyone can decide what they want to post about such as: their beliefs, organizational news, events, and media. (Zelin, 2013).

Brief History of ISIS and Use of Social Media

This move to social media, especially to real time posting platforms, has been highly reported on by news outlets such as *CNN*, *BBC*, and *The Atlantic*, and academics such as Gabriel Weimann. No group to date seems to have made the move, and made it quite as successfully as the Islamic State of Syria and Iraq (ISIS) (Nissen, 2014). The history of ISIS can perhaps explain how they have been so successful in using social media platforms. The roots of ISIS began in 2004 as a splinter al-Qaeda group in Iraq (Stern & Burger, 2015). This group, which was at the time known as al Qaeda in Iraq, began to amass power as it disseminated its Islamic ideology and also began crafting a strategic plan to power. In 2006, al Qaeda in Iraq's leader, Abu Ayyub al-Masri, announced the creation of the Islamic State of Iraq (ISI) (Weiss & Hassan, 2015). By 2010, the leader of this new group, Abu Omar al-Baghdadi, was killed during a U.S.-Iraqi operation, and the current leader, Abu Bakr al-Baghdadi, came into power. In the years that followed, al-Baghdadi oversaw the expansion of ISI into Syria as ISI took advantage of the Syrian Civil War to declare a merger with an al Qaeda backed group in Syria known as the al-Nusra Front (CNN, 2014). The merger of these two groups resulted in what we now know as ISIS (or, as al-Baghdadi proclaimed, Islamic State in Iraq and the Levant (ISIL)). This merger, however, was not agreed upon by the al-Nusra Front, and al Qaeda soon broke ties with ISIS. In 2014, ISIS, led by al-Baghdadi, proclaimed the creation of a Caliphate and changed their name to the Islamic State. This history spans the years that social media itself was coming to the forefront of web technologies. As

Ryan (2014) expresses in her article on how ISIS and al Qaeda use Twitter and other social media differently, ISIS attempts to propagandize "young, disillusioned Westerners who are ripe for radicalization," and who are seeking a sense of community (p.2). Twitter, Facebook, and Youtube are prime tools for this because they reach a much younger audience. Ryan also notes that al Qaeda still focuses mostly on the older style websites and forums. These were the "hot" new technologies when al Qaeda first came around to using them, but much of the media attention has moved away from the older styles to the new social media platforms. ISIS uses this new attention on social media platforms to generate attention for themselves.

This attention to campaigning on social media has been called "sophisticated" by multiple reputable sources in the media such as the BBC (2014), the Atlantic (2014), and Time (2014), and by academic scholars and researchers such as Weiss and Hassan (2015), Stakelbeck (2015), Providence Research (2015), and Hall (2015). This social media campaign focuses on demonstrating a single goal (the Caliphate) and a common purpose towards attaining this goal (Nissen, 2014). Nissen (2014), of the Royal Danish Defense College, also notes that ISIS has formed a narrative around this single goal and places a "shared" history on it in order to entice more followers into the fold. This narrative is that a singular Caliphate marks the return to the original Islam and as such, the Islamic State offers a "utopian Muslim universalism" that does not make distinctions about a person except their "degree of zealotry" (Hussein, as cited by Nissen, 2014, p.2). By forming this singular goal with a singular narrative, ISIS can place themselves as the underdog in a world that is against them; they can become the heroes simply fighting for

their homeland rather than disillusioned men savaging and destroying countries and people.

ISIS, Propaganda, and Twitter

While ISIS makes plenty of use of other social media platforms to project this "underdog" campaign, much of the campaigning centers on Twitter. Within this social media platform, ISIS has a distributed hierarchy to disseminate information and drum up support. This hierarchy starts with the official top-down administration as seen in older terrorist websites, but then goes down to supporters or sympathizers who may not even be officially part of, or even fighting for, ISIS (Nissen, 2014). The central administrators provide more polished video content, important news or ideological facts, and then this gets re-tweeted over and over as it makes its way out into the "Twittersphere." The more outside supporters and the militants provide information about how "peaceful" life in the Islamic State is, how they wish they could go and wage jihad, how the jihadists are in the right, and then more mundane details simply telling about their lives or sharing information about their cats (Zelin 2013; Speri, 2014; Stone, 2014).[ii] It is this network amongst actual jihadists, supporters, sympathizers, and simply those looking for a community or interested in the movement that makes Twitter such a valuable instrument for ISIS. As items get retweeted, and more connections made, ISIS has the greater ability to expand their network beyond their own physical borders.

In order to expand its network, ISIS not only uses Twitter but also "games" it. ISIS released an Arabic-language Twitter app known as The Dawn of Glad Tidings (supposedly defunct as of December 2014), that was readily available in the Google Play Store (Berger, 2014). This app would post tweets to your account as well to the accounts

of all those who had signed up for the app. The amount of tweets this one application sent out would cause some hashtags or Tweets to be "trending" on Twitter, and thus gain more attention and more followers. On top of this, ISIS spaced out the tweets enough to avoid setting off Twitter's spam-detection algorithms (Berger, 2014). Spacing the tweets out, and developing the app to begin with, shows a high level of sophistication and knowledge of the programming behind Twitter itself. Along with developing an app to game the infrastructure of Twitter, ISIS has also been known to hijack harmless hashtags and use them for their own propaganda. Peter Van Praagh, president of the Halifax International Security Forum had to issue a statement on November 22, 2014, about ISIS's hijacking of the Forum's hastag "#HISF2014" (Van Praagh, 2014). ISIS had used the hashtag to circulate a video of a British captive and to send messages to other participants and members of the Forum. Hijacking hash tags, developing apps, and avoiding spam detection are signs that ISIS is well aware of the audience Twitter reaches as well as the infrastructure of Twitter itself

---

NOTES:

[i] While Facebook was founded earlier than 2006, it only became open to the general public in 2006 (Facebook, 2014).

[ii] It should be noted that while cats are considered "the social media cliché par excellence" (Speri, 2014), ISIS fighters and supporters most likely are trying to imitate Abu Huraira, a companion of the Prophet who had an extreme fondness for cats (al Janabi as cited by Speri, 2014). Still, cats on a social media account are more likely to attract attention and draw people in than a picture of a gun.

METHODOLOGY

General Methodology

This research used quantitative methods in order to answer the Research Questions. Quantitative data allows for more accurate predications to be made and verified (Johnson & Christensen, 2013) while also adding to the larger picture of the overall data. A quantitative approach also allows the research to gain a more clearly objective and statistically valid study (Anderson, 2006). Due to the amount of data gathered, an overall quantitative approach was considered the best and most reliable method for gathering and studying the necessary data.

Research Design

This research used data mining tools that allowed data to be collected directly from the source, in this case Twitter. This kind of research design was best suited to collect this kind of data because it gave the researcher a chance to collect primary data directly from the online community without having to interact with individual Twitter users. Since the research questions above are best answered by a bird's eye view of the data, and not from one-on-one interaction, gaining the bigger picture was more important to the overall research. The best way to gain this bigger picture was through Twitter's own APIs, both streaming and search. Through these APIs, the researcher was able to access a lot of data over different time periods and in reaction to different events.

Sample Size and Sampling

The sample frame for this research was all Twitter users who tweeted a specific hashtag or keywords during a specified time frame in relation to a critical incident. The time frame chosen was based on "critical incidents." Critical incident is a term that has been used over the past several decades to represent the psychological study of people and cultures (Flanagan, 1954), which is more formally known as the Critical Incident Technique. More recently, the term has also been used for Critical Incident Analysis (CIA) (Schwester, 2011). It is this last term that pertains to this research: A critical incident is any event that creates a "theater of action," to which individuals respond. In this research, the critical incident pertains to any event that ISIS used to draw attention to themselves because this creates the "theater of action" as outlined by Schwester (2011). These incidents then spawned hashtags, keywords, or urls that ISIS members and supporters would then use to spread their propaganda through Tweets. Since the data collected was in response to these critical incidents, there was no set sample size, only however much data could be collected through the Twitter APIs. This response means that there are two constraints on the data: 1. The focus is on the response itself, not on a certain set of actors, and 2. The constraint on data collected by the APIs.

The sampling occurred by accessing both the Streaming and Search Twitter APIs and specifying the specific hashtags and keywords used by ISIS followers and supporters. Both APIs were used because the Streaming API can collect real-time data, but is unable to collect past data whereas the Search API can collect up to seven days worth of data. By having both APIs available, it means that a better overall and more precise collection of data could occur. It also means that if the results from one API follow a pattern and then

the other API results follow the same pattern, there is a greater degree of certainty that the overall network structure follows a specific pattern. If the results from the APIs are different, then more research will be needed to determine why there are differences and why these differences result in a different network structure for the same hashtags and keywords. These hashtags and keywords were manually determined as videos or new propaganda was released through social media. While some videos and materials were widely circulated among followers and supporters using certain keywords, others were hard to ascertain what the keyword or hashtag would be, causing a loss in data collection. O'Callaghan, Prucha, Greene, Conway, Carthy, and Cunningham (2014) acknowledge that for ongoing conflicts, especially those that are less established in terms of the actors, data is lacking in the phrases that groups consistently use to propagate their materials. This is especially true with ISIS followers and supporters who want to actively promote propaganda but also have to constantly bring their accounts back up when Twitter suspends them for their propaganda. The sampling, and as a consequence, the sample population, are a direct result of the manually chosen keywords. If the keyword chosen was not as popular with the followers and supporters as previous keywords, less data was collected. A specific example of data collection process can be found in Appendix 1.

Research Method

Social Network Analysis

To analyze the data gathered from ISIS's propaganda on Twitter, the researcher used tools from Social Network Analysis. Social Network Analysis is a type of study that seeks to determine and understand the underlying network structure within a social group (Scott, 2012). It was not originally developed for technical platforms, but has

slowly evolved as a way to analysis big data that results from many social media platforms. Social Network Analysis is best suited for data that arises from a "community structure," and from "relational data" that shows connections from one member to another (Scott, 2012, p.3). Twitter data fits into these categories because the communications show relation from one Twitter user to another, and it also shows the underlying community structure of the larger group. Social Network Analysis looks at factors such as nodes, edges, centrality, and clustering, and uses mathematical algorithms and statistics to discover patterns made of these factors (Cook & Holder, 2006; Knoke, 2008). Using Social Network Analysis tools on ISIS Twitter propaganda data helped in answering the research questions relating to ISIS's Twitter network.

Research Tools

This research employed many tools in order to gain access to the necessary data, and then later for parsing and analysis. The first tools used were the Twitter Streaming and Search APIs. The Twitter Streaming API was accessed by using a Python library called Tweepy (Moujahid, 2014). A Python script was created that imported the Tweepy library, authenticated and connected to the Twitter Streaming API, and filtered the Twitter Streams using specific keywords. The filtered Twitter Streams return all matching Tweets as long as the volume of Tweets is below or equal to the streaming cap (Twitter, 2015). This means that the Python script should return all tweets matching the specific keywords unless the volume is such that Twitter's rate limits are breached. Research has shown that most Streaming API users are only receiving about 1% to 40% of all specified tweets (Bright Palnet, 2013). The Twitter Streaming API is also only capable of collecting data as it happens. This means that if someone's tweet matched a

keyword, but it was tweeted before the Python script was set running, then that tweet will not be included in the final data collection from the Streaming API.

The Twitter Search API was accessed using NodeXL's import Twitter data feature. NodeXL, a free, open-source template for Microsoft Excel developed by the Social Media Research Foundation (2015), queries the Twitter Search API for specified keywords when the user chooses to import Twitter Search Data. The Twitter Search API lacks the completeness of data from the Twitter Streaming API because it is focused on relevance not completeness (Twitter, 2015). Due to this focus, less tweets will be gathered than even the Streaming API. However, the Twitter Search API does allow for collection of data from up to 7 days previous to the search. In practice, this means that an import Twitter search query run through NodeXL can produce older tweets than that found from the Twitter Streaming API. Both of the APIs were used in an effort to gain a more complete picture of how ISIS spreads their propaganda on Twitter.

Other tools used were a Python script developed to parse through the data output from the Twitter Streaming API. Since the Twitter Streaming API outputs it data in the JSON data format, it could not simply be opened in Excel and run through the NodeXL template. Instead, the Python script searched each line of the JSON data, found the matches for a specific keyword, and then outputted that data to a text file. This text file was then opened in Microsoft Excel, manually perused and formatted to ensure the highest quality of data, and then imported into NodeXL. The data collected through NodeXL itself from the Twitter Search API was already formatted properly.

Data Analysis and Presentation

The collected data was analyzed using NodeXL's built-in visualization features and mathematical formulas. The data was analyzed using in-degree, out-degree, closeness centrality, and betweeness centrality. Data is not only presented as these statistics but takes advantage of the visualization component built-in to NodeXL to visually represent the social network of ISIS's followers and supporters. The visual network along with the statistical metrics best represents the data necessary to answer the research questions about dissemination of data, centrality of nodes, and network structure. The data metrics collected from each separate critical incident were compared to each other in order to see the overall network structure and to ascertain the dissemination of ISIS propaganda material.

FINDINGS

The results from the Twitter data are broken down into three different critical incidents: 1. The beheading of Japanese Hostage, Kenji Goto, released January 31st, 2015, 2. The burning alive of the Jordanian Pilot, Moaz al-Kasasbeh, released February 3rd, 2015, and 3. The release of the online ISIS magazine, Dabiq, on February 12th, 2015. These three events represent critical incidents because they were catalysts for theaters of action and reaction (Schwester, 2011). The first critical incident – the beheading of Kenji Goto – resulted in not only mass condemnation of ISIS from the nation of Japan and other allies but also resulted in mass suspension of pro-ISIS Twitter accounts by Twitter (Vocativ, 2015). The immolation of Moaz al-Kasasbeh resulted in a further Twitter crackdown, and in the country of Jordan beginning airstrikes against ISIS territories (Broder, 2015). Both of these events belong in the class of propaganda because ISIS used these events to show strength and might in order to motivate people towards their cause. As Farwell (2012) notes, violent propaganda can be used to disturb a regime and show that victory is possible. The violence is also being used by ISIS to show their "degree of zealotry" for bringing about a more perfect Islam (Hussein, as cited by Nissen, 2014, p.2). However, this violence has to be counter-balanced with a narrative of hope and substance (Farwell, 2012). This hopeful narrative can be seen in the release of *Dabiq*. *Dabiq* is a periodical magazine that focuses on life inside ISIS territory as well as on the ideology behind the formation of the Caliphate (The Clarion Project, 2014). While boasting or dispensing words of wisdom, *Dabiq*'s overall goal is to paint a romantic

portrait of what life inside the Caliphate can be, and to show how the Caliphate exemplifies the "utopian Muslim universalism" of original Islam (Hussein, as cited by Nissen, 2014, p.2). This romantic portrait is then used to draw in people outside of the Caliphate borders and to get a larger audience to support ISIS's ideology. By focusing on two violent incidences and one non-violent incident, this research attempted to gain a better-rounded view of how ISIS disseminates their propaganda, both violent and hopeful.

The critical incidents were further broken down into how information was gathered. For Critical Incident 1, both the Streaming and Search APIs were used to collect data that matched the keyword "A message to the government of Japan." For Critical Incident 2, the Streaming API was used to collect data that matched the keyword "Healing of the Believers' Chests." Finally, Critical Incident 3 was captured using the Search API through NodeXL.

Measurements

In order to accurately report the findings, the measurements on the data should be discussed. The measurements were collected using built-in features of NodeXL. The metrics used to analyze the data include: In-degree, Out-degree, Betweenness Centrality, and Closeness Centrality. These three metrics have arisen from network analysis as a way to best get at the nodes that are more central than others (Freeman, 1978).

Degree Centrality

Both in-degree and out-degree are measures of connections between two vertices (nodes) within the data. In-degree measures the amount of connections that point towards (inward to) a vertex (Hansen, Shneiderman, & Smith, 2010). For Twitter data,

this in-degree measures how many tweets are directed at a person. This direction can include a reply-to or mention from one user to another. If @sally1234 mentions @bob5678, then @bob5678 has an in-degree of 1 because he has received a connection that points towards him. Out-degree measures the opposite of in-degree in that it counts how many times a connection starts at a vertex and points outwards towards other vertices (Hansen et al., 2010). For Twitter data, this means tweets going out from the original user. In the example given above, @sally1234 would have an out-degree of 1 because she tweeted from herself to @bob5678. The point originated with her vertex point and then connected to the other vertex. For tweets that are not directed at anybody and only originate from the source, the in-degree and out-degree will be equal. This means that if @sally1234 had simply tweeted a message with not mention or reply to another Twitter user, then her in-degree and out-degree score would both be 1.

Betweenness Centrality

Betweenness centrality measures how central a node is to a network by computing "how often a given vertex lies on the shortest path between two other vertices" (Hansen et al., 2010, p.40; Newman, 2003). The final betweenness score will show how important a particular node is to the network because it shows how strong of a bridge it is for information to pass through. If a node has a particularly high betweenness score, then that means that it is a very strong bridge within the network; it helps to connect nodes to each other in order to continue passing along information. A node with a high betweenness score may act as a "gatekeeper" (Bruggeman, 2013, p.133) because information diffuses through it.

Closeness Centrality

Closeness centrality measures how close one vertex is to other vertices by averaging the distance between a vertex and all the other vertices in the network (Hansen et al., 2010; Okamoto, Chen, & Li, 2008). There are different algorithms for closeness centrality with the "simple closeness" being simply the inverse measure of centrality (Bruggeman, 2013). This means that the larger a number, the further away from the center it is. "Normalized closeness" attempts to make the range of closeness be from 0 to 1 in order to correlate larger values with greater centrality. NodeXL's equation for closeness centrality normalizes the closeness, but it keeps with the smaller number being more centrally located instead of taking the inverse (Hansen et al., 2010).

Critical Incident 1

Critical Incident 1 refers to the release of footage showing the beheading of Japanese hostage Kenji Goto. The video was released by Al-Furquan Media, the known media wing of ISIS, on January 31st, 2015. The researcher reviewed Twitter accounts of stated ISIS affiliates and determined that "A message to the government of Japan" was being used as a pro-ISIS phrase for the dissemination of the video.

Streaming API

After the key phrase was determined, the researcher then inputted this key phrase into the Python API script and set the script to running. The script ran for over 48 hours, however, after the initial 48 hours, the key phrase had been picked up by media and was resulting in irrelevant data. Thus the results for the Streaming API are for a 48-hour span starting at 5:15pm on January 31st, 2015.

The script for the Streaming API resulted in 644 vertices (nodes) with 600 unique edges (relationships), 69 edges with duplicates (meaning the vertices tweeted along the

same path), and a total of 669 total edges. There were also 251 self-loops, which occur when a user tweets without replying to or mentioning another user so it simply forms a self-loop of input-output.

In-Degree. The top 20 users with the highest In-Degree Centrality were chosen for representation. These are the users that tweeted the most information out to other people.

Table 1

Highest In-Degree Centrality Amongst Twitter Streaming API Results for Critical Incident 1

Vertex	In-Degree
Abdul_aliy_3	77
IslamforEA5rica	51
tkatsumi06j	24
hassan_japan	21
jtshibata3	20
bigkottakromac	20
Almahira__	17
fisfisso	12
abothar1000	12
aajtak	11
salah_news4	10
dokka_umaroov	7
Yde2015123	7
rocks_31	7
garfy_hattan	7
2_howdawl	6
katayan1111	6
abo_hazem1436	5
syufuru	5
suger_and_solt1	5
abukhalid4dwlh	5

Out-Degree. The top 20 users with the highest Out-Degree Centrality were chosen for representation. These are the users that received the most tweets from other users.

Table 2

Highest Out-Degree Centrality Amongst Twitter Streaming API Results for Critical Incident 1

Vertex	Out-Degree
AbuAlbaraOtb	7
2_howdawl	5
JMSHYYD	5
AAlbadriy	4
anas__2015	2
harus_belajar	2
beastofislam85	2
losttimememoryr	2
chiblalkhalifa	2
karwan8787	2
abo_moawia_ly	2
ii51000	2
YUKARING1222	2
ryu3g3	2
Warior1924	2
con30078	2
Abdul_aliy_3	1
tkatsumi06j	1
hassan_japan	1
bigkottakromac	1
Almahira__	1

Betweenness Centrality. The top 20 users with the highest Betweenness Centrality Score were chosen for representation. These are the users that acted most as gatekeepers and bridges for the information. The higher their betweenness score, the more data that passes through them.

Table 3

Highest Betweenness Centrality Amongst Twitter Streaming API Results for Critical Incident 1

Vertex	Betweenness Centrality Score
Abdul_aliy_3	5700.000
IslamforEA5rica	2550.000
dokka_umaroov	1482.600
AbuAlbaraOtb	1305.400
fisfisso	890.000
salah_news4	882.000
karwan8787	858.000
JMSHYYD	585.600
Yde2015123	578.200
tkatsumi06j	506.000
hassan_japan	456.000
abo_moawia_ly	450.000
jtshibata3	380.000
Cant_Stop_IS	378.000
bigkottakromac	342.000
alanbar_spring	288.000
abo_hazem1436	288.000
AAlbadriy	253.000
Almahira__	240.000
abothar1000	110.000
ii51000	98.000

The influence of these vertices can be seen in Figure 1. The solid circle represents user Abdul_aliy_3, who has the highest betweenness centrality score. The solid diamonds represent the rest of the top 20 as well as any users who have a between centrality score of greater than 1. All other users have an empty circle.

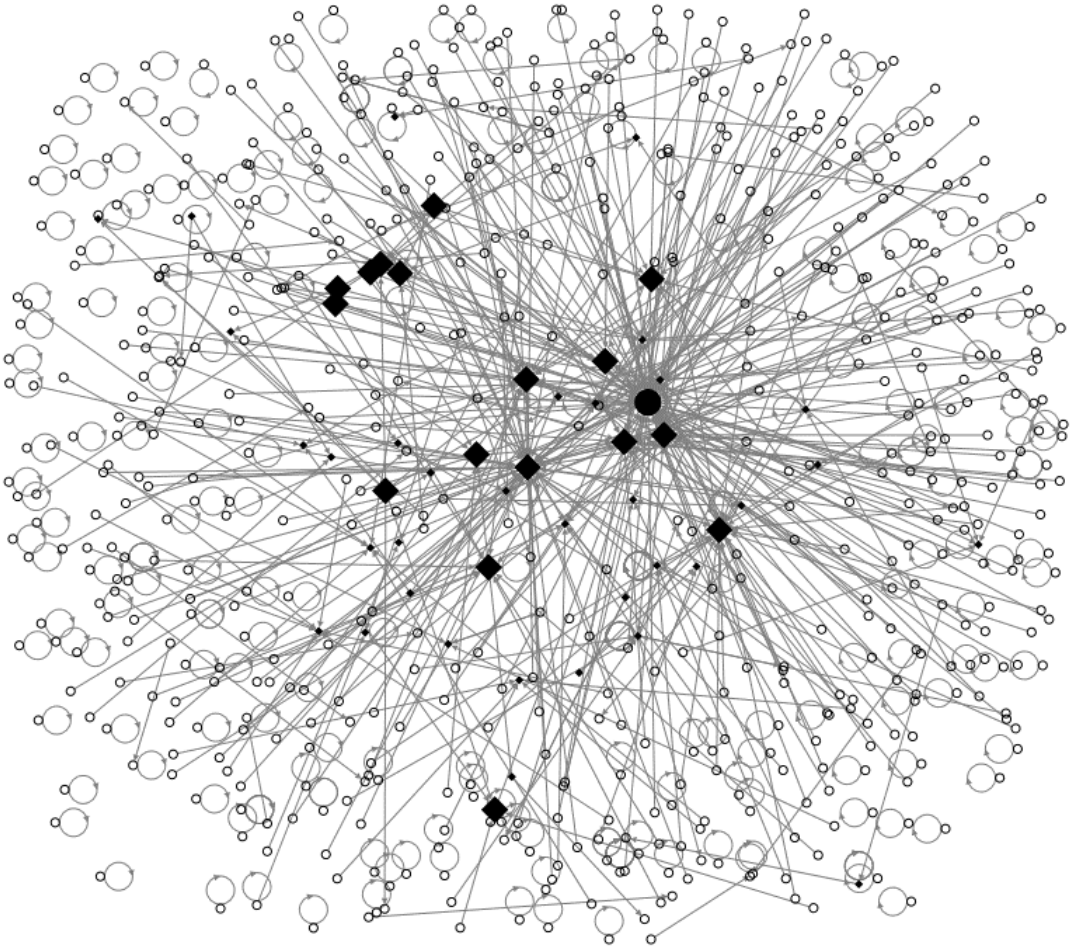


*Figure 1.*Visualization of the betweenness centrality scores for Critical Incident 1 using the Twitter Streaming API. This figure illustrates the highest betweenness centrality scores amongst the data.

As seen in Figure 1, the nodes with the highest betweenness centrality scores help to connect other nodes to each other. They represent the center of a hub through which information flows. And, while there is a highest betweenness centrality score, there are other nodes that act as hubs for other users.

Closeness Centrality. Closeness centrality is not a metric that can accurately be depicted simply by showing the top 20 users with the lowest metric score. All of the top 20 would have a closeness centrality score of 0 because it was a tweet from the user to

nobody else. It was not a mention or reply to, so there is no other vertex for which the originating vertex to be close. The best way to show closeness centrality is to show the overall metrics for the network.

Table 4

Overall Scores for Closeness Centrality for Critical Incident 1 From the Twitter Streaming API

Type	Result
Minimum Closeness Centrality	0.000
Maximum Closeness Centrality	1.000
Average Closeness Centrality	0.133
Median Closeness Centrality	0.010

Results for Critical Incident 1, Streaming API. The results from the measures of centrality show that those with the largest In-Degree scores (Table 1) correspond to those with the largest betweenness scores (Table 3), and that the network overall is fairly close together with an average closeness centrality score of .133 (Table 4). The 2 users with the highest in-degree scores also have the 2 highest betweenness scores. Based on what each of these measures of centrality mean, it points towards these two users being the bridges through which most information passes. User Abdul_aliy_3 only tweeted out once, but this tweet was then taken up and mentioned in 77 other tweets. This points towards Abdul_aliy_3 being someone important within the network structure, or at least someone who is able to get information more quickly than some of the others.

Figure 1 visualizes how these most-connected nodes work together to form the overall network structure. The solid diamonds represent the nodes with higher betweeness scores, and the solid circle represents the user with the highest betweenness score, user Abdul_aliy_3. Many of the users with high betweenness scores appear to be very connected with the center few being more closely connected than those along the

periphery. Figure 1 also shows that the network is close together. With an average closeness score of .133, the overall distance of path for each user is short. Many of the users are close to the central hubs of information.

For this network, tweeting a lot (which results in a higher in-degree) did not matter as much as how often one of the user's tweet was mentioned (resulting in a higher out-degree). This pattern means that one tweet from a well-placed user is more important to the dissemination of information than having multiple users tweet the same thing and then never having that message picked up, as can be seen with the number of self-loops that go nowhere and do not add to the overall information structure.

Search API

The Search API was accessed using NodeXL's import from Twitter feature. It searched for the key phrase, "A Message to the Government of Japan," and was limited to just over 150,000 tweets. The import was started a little after 6pm on January 31st, 2015, and ran until mid-afternoon the next day.

The import from the Twitter Search API resulted in 595 vertices (nodes) with 1595 unique edges (relationships), 116 edges with duplicates (meaning the vertices tweeted along the same path), and a total of 1711 edges. There were also 110 self-loops.

In-Degree. The top 20 users with the highest In-Degree Centrality were chosen for representation. These are the users that tweeted the most information out to other people.

Table 5

Highest In-Degree Centrality Amongst Twitter Search API Results for Critical Incident 1

User	In-Degree
erhabee_p	40
cant_stop_is	37
mousaalomar	29
kkansaa1	27
salah_news4	26
kn___mo	25
tumedia85	24
dydx198	22
n__q__kh	20
o111492	19
h_963_h	19
mezzni07	18
dokka_umaroov	18
hatrek_3	17
vovovovo1414	15
iiiiiii990	14
saqr344	14
alansarialmhajr	13
asmmoo2015	13
abom7md103	12
is_omar88	12

Out-Degree. The top 20 users with the highest Out-Degree Centrality were chosen for representation. These are the users that received the most tweets from other users.

Table 6

Highest Out-Degree Centrality Amongst Twitter Search API Results for Critical Incident 1

User	Out-Degree
mezzni07	92
eslam70073612	43
asud_alswarm	26
muslim966	23
saerr3dd	21
bnt_abay	20
iiiiiii990	18
egypt1angel	18
alansarialmhajr	16
ssqqggsss	16
98ad61d32ee64aa	16
omubaker11	15
ibbbcj7	15
twasswarti	15
dmera5588	13
isisarap	13
4soaadh	12
dolawy22	12
thenativeboy	12
alkinga46	11
rehamis009	11

Betweenness Centrality. The top 20 users with the highest Betweenness Centrality Score were chosen for representation. These are the users that acted most as gatekeepers and bridges for the information. The higher their betweenness score, the more data that passes through them.

Table 7

Highest Betweenness Centrality Amongst Twitter Search API Results for Critical Incident 1

User	Betweenness Centrality
mezzni07	94597.103
ibbbcj7	35879.602
cant_stop_is	27985.223
cnfj	27104.323
youtube	21706.337
eslam70073612	20743.302
erhabee_p	19096.920
mousaalomar	18952.327
giboccir	16398.639
islamforea5rica	16219.396
ohnojunichi	14419.413
2_howdawl	14007.912
abdiwaahid	13088.309
suwasamurai	12919.905
kkansaa1	12064.876
toshio_tamogami	11739.101
m_media_news	11510.333
iiiiiii990	10630.524
tokyo_laurel	10620.191
hatrek_3	10505.261
kohf77	10438.702

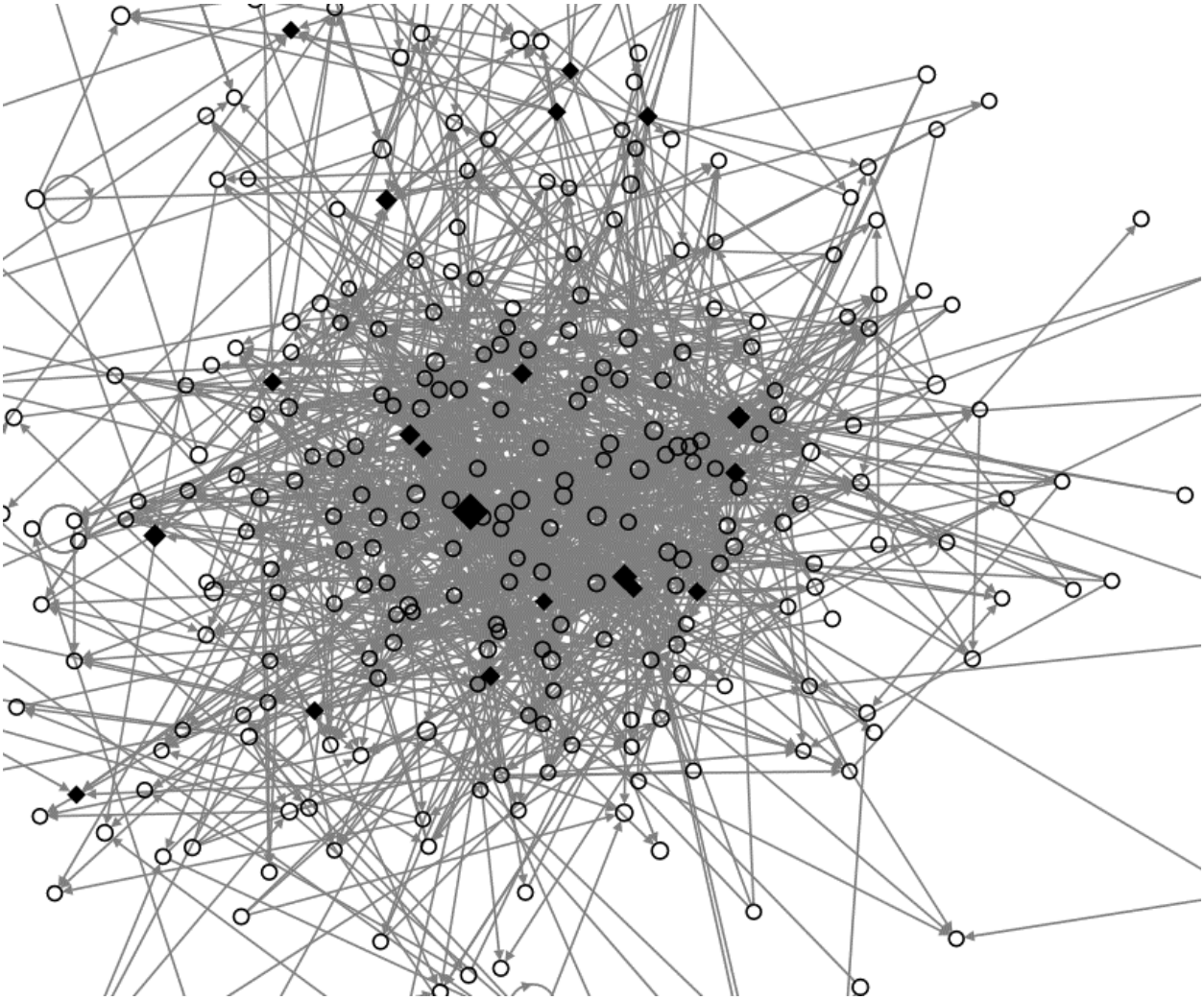


Figure 2. Visualization of the betweenness centrality scores for Critical Incident 1 using the Twitter Search API. This figure illustrates the highest betweenness centrality scores amongst the data.

Closeness Centrality. Closeness centrality is not a metric that can accurately be depicted simply by showing the top 20 users with the lowest metric score. All of the top 20 would have a closeness centrality score of 0 because it was a tweet from the user to nobody else. It was not a mention or reply to, so there is no other vertex for which the originating vertex to be close. The best way to show closeness centrality is to show the overall metrics for the network.

Table 8

Overall Scores for Closeness Centrality for Critical Incident 1 From the Twitter Search API

Metric	Results
Minimum Closeness Centrality	0.000
Maximum Closeness Centrality	1.000
Average Closeness Centrality	0.024
Median Closeness Centrality	0.000

Results for Critical Incident 1, Search API. This network differs from the Streaming API results to Critical Incident 1 in that both in-degree (Table 5) and out-degree (Table 6) matter when it comes to having a higher betweenness score (Table 7). Both the highest-ranked user for in-degree and the highest-ranked user for out-degree appear in the top 20 betweenness centrality scores. User mezzni07 (the user with the highest out-degree score at 92) still had a higher betweenness score than those users with high in-degree scores, but the overall results are not as cut and dry as those from the Streaming API for Critical Incident 1. This means there was an overall larger flow of information with many of the information gatekeepers being originators of information (in-degree) just as much as they were receivers of information (out-degree).

This more consistent in-and-out flow of information amongst sets of the same users also results in a lower average closeness centrality score of .024 (Table 8). This is visible in Figure 2 because the network as a whole appears more tightly clustered together. In Figure 2, the solid diamonds represent the users with higher betweenness scores with the larger the diamond correlating with the larger betweenness score. The largest solid diamond is user mezzni07 with a betweenness score of 94597.103.

This network pattern means that users who both tweet themselves and then have those tweets picked up in mentions and reply-tos are just as important as those that

receive all the mentions and reply-tos. In this network, information is passed back and forth rather than just picked up and carried on as in the network for Critical Incident 1, Streaming API. While the networks between Streaming API and Search API are similar in vertices size (644 and 595), the search API resulted in a larger overall-connected network structure with 1711 edges compared to only 669 from the Streaming API. These results may have occurred because the Search API was able to pick up more tweets right at the start of the critical incident since it is capable of going up to 7 days in the past while the Streaming API was only able to pick up tweets once the script was started, and even then, it had to abide by the rate limits resulting in a loss of information.

Critical Incident 2

Critical Incident 2 refers to the release of footage showing the immolation of Jordanian hostage Moaz al-Kasasbeh . The video was released by Al-Furquan Media on February 3rd, 2015. The researcher reviewed Twitter accounts of stated ISIS affiliates and determined that "Healing the Believers' Chest" was being used as a pro-ISIS phrase for the dissemination of the video.

Streaming API

After the key phrase was determined, the researcher inputted the key phrase into the script and ran the script for the next 4 days. The script was started at 6pm on February 3rd, 2015. This was a small time after the video had been released, but the researcher was unable to remotely access the script and set it running. Even though the script ran for 4 days, not as many tweets were picked up as for the Japanese hostage.

The script for the Streaming API resulted in 45 vertices (nodes) with 40 unique edges (relationships), 6 edges with duplicates (meaning the vertices tweeted along the same path), and a total of 46 edges. There were also 12 self-loops.

In-Degree. Due to the smaller amount of vertices, only the top 10 users with the highest In-Degree Centrality were chosen for representation. These are the users that tweeted the most information out to other people.

Table 9

Highest In-Degree Centrality Amongst Twitter Streaming API Results for Critical Incident 2

User	In-Degree
9ariban_9ariban	21
10JihadiA	4
Mdina_Sanorji3o	3
osidosid27	3
hor_aljana	2
AimanHkim	2
_antijewish	1
Umah_Way	1
O_O260	1
Hosni0812A	1
dawlh433	1

Out-Degree. Due to the smaller amount of vertices, only the top 10 users with the highest Out-Degree Centrality were chosen for representation. These are the users that received the most tweets from other users.

Table 10

Highest Out-Degree Centrality Amongst Twitter Streaming API Results for Critical Incident 2

User	Out-Degree
9ariban_9ariban	1
osidosid27	1
hor_aljana	1
AimanHkim	1
_antijewish	1
O_O260	1
Hosni0812A	1
dawlh433	1
lIlIlllIlIlllI	1
ArchivePress2	1
ZahranKitty2	1

Betweenness Centrality. The top 10 users with the highest Betweenness Centrality Score were chosen for representation. These are the users that acted most as gatekeepers and bridges for the information. The higher their betweenness score, the more data that passes through them.

Table 11

Highest Betweenness Centrality Amongst Twitter Streaming API Results for Critical Incident 2

User	Betweenness Centrality Score
9ariban_9ariban	456.000
hor_aljana	82.000
10JihadiA	12.000
Mdina_Sanorji3o	6.000
osidosid27	2.000
AimanHkim	0.000
_antijewish	0.000
O_O260	0.000
Hosni0812A	0.000
dawlh433	0.000
lIlIlllIlIlllI	0.000

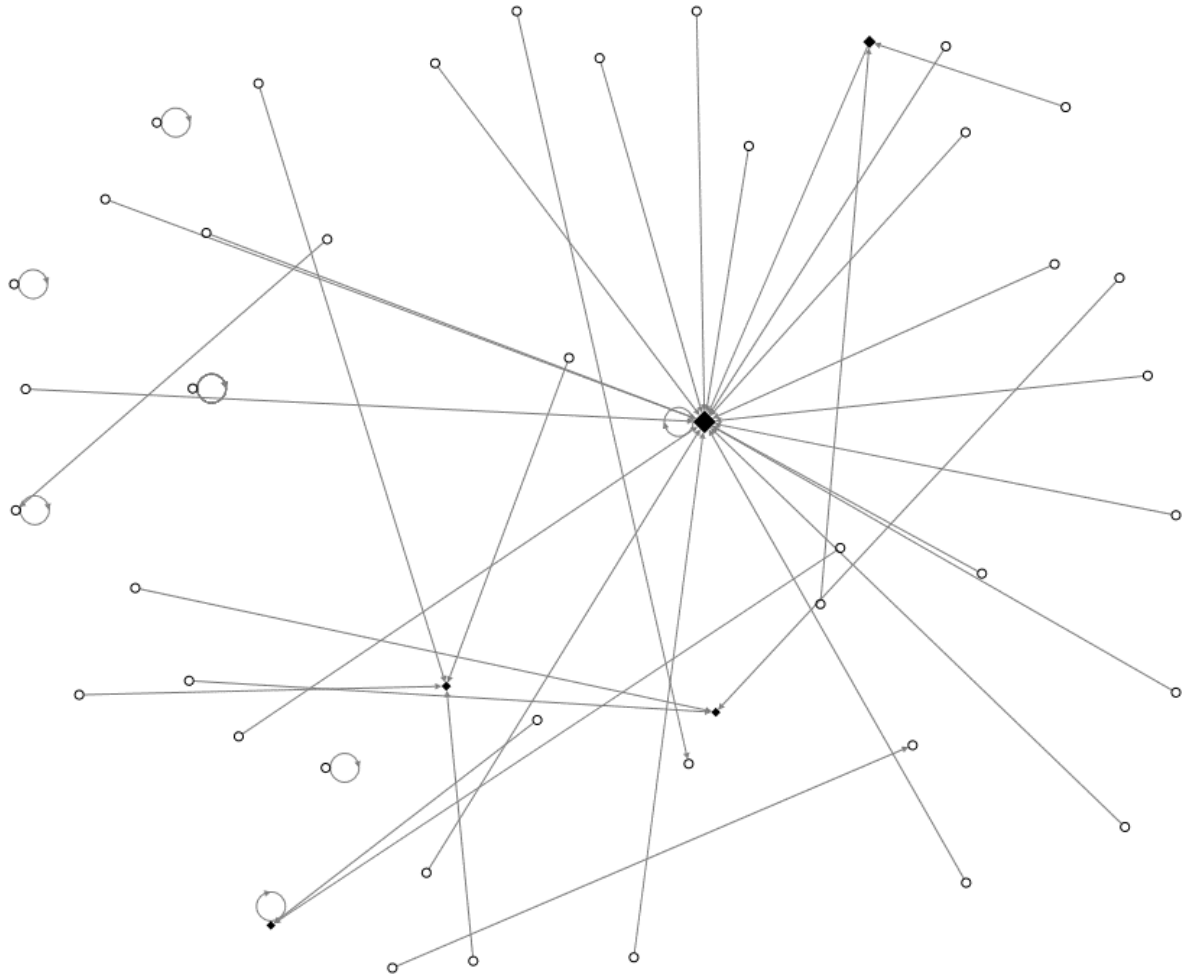


Figure 3. Visualization of the betweenness centrality scores for Critical Incident 2 using the Twitter Streaming API. This figure illustrates the highest betweenness centrality scores amongst the data.

Closeness Centrality. Closeness centrality is not a metric that can accurately be depicted simply by showing the top 10 users with the lowest metric score. All of the top 10 would have a closeness centrality score of 0 because it was a tweet from the user to nobody else. It was not a mention or reply to, so there is no other vertex for which the originating vertex to be close. The best way to show closeness centrality is to show the overall metrics for the network.

Table 12

Overall Scores for Closeness Centrality for Critical Incident 2 From the Twitter Streaming API

User	Closeness Centrality Score
Minimum Closeness Centrality	0.000
Maximum Closeness Centrality	1.000
Average Closeness Centrality	0.210
Median Closeness Centrality	0.022

Results for Critical Incident 2, Streaming API. These results show that the user with the highest in-degree score (Table 9) resulted in the highest bewteenness score (Table 11). However, this network was also not as tightly-knit as the other previous two. With an average closeness centrality score of .210 (Table 12), the users are not very far away, but they are still further away from each other than those in Critical Incident 1.

This network pattern shows that much of the information is disseminated through one user, 9ariban_9ariban tweeting out to other users. The visualization in Figure 3 uses solid diamonds that correspond in size to higher betweenness scores. As seen in Figure 3, there is really only one user with a high betweenness score and the other users seem to exist only on the periphery. There does not appear to be overall much interaction amongst the users. This network is also much smaller than the other 3 considered in this section. Even though the Streaming script ran for the same, if not more, time than the Streaming script for Critical Incident 1, there was just not as much happening on Twitter. There could be a few reasons for this. One, this came on the tail end of Critical Incident 1 with the two overlapping in time. Since Critical Incident 1 was a bigger media event, it could have impacted how focused ISIS supporters were on any other events. Secondly, the researcher could have chosen the wrong key phrase. If ISIS supporters started to use

another key phrase to spread their news, then the script would not have picked that phrase up, resulting in a loss of information. Third, not long after the release of the immolation video, King Abdullah II vowed a "relentless war" against ISIS (aawsat.net, 2015). The video was released on February 3rd, 2015, and soon after the release news began circulating that Jordan would probably react in a strong way to the video. This news, and a possible impending airstrike from the country of Jordan, may have been more at the top of ISIS supporters' minds than simply spreading the video. All three of these reasons could have resulted in an overall smaller network.

Critical Incident 3

Critical Incident 3 refers to the release of ISIS's English-language magazine, *Dabiq*. The magazine was released online on February 12th, 2015 (talkleft.com, 2015). Its title was "From Hypocrisy to Apostasy: The Extinction of the Grayzone," and it included an interview with British hostage John Cantile. It also featured an interview with Hayat Boumeddience, the wife of Amedy Coulibaly, the Paris kosher supermarket attacker (pjmedia.com, 2015). The researcher reviewed the news releases and then searched through Twitter to see how the pro-ISIS cohort was spreading the news of the release. "Dabiq" appeared to be the way most pro-ISIS supporters were spreading the news.

Search API

After the keyword was determined, the researcher waited 24 hours, until February 13th 2015, to input the keyword into the "import Twitter data" feature in NodeXL. This feature backends into Twitter' Search API and can find data from the last 7 days. The reason for waiting 24 hours was to allow more information to disseminate across Twitter.

Once the data collection process was through, the researcher noticed there were a lot of false positives in the data. The Twitter user would use the term "Dabiq," but would only be reporting it from a news agency standpoint, or in some cases, as outrage that the magazine had been released at all. To remove these false positives, the researcher filtered the results to only those that used an archive.org url within their post. Since the magazine is inflammatory and acts a terrorist handbook in many ways, most sites block access to the link once the site releases what it actually is. This mean that any links of the magazine on Twitter had a greater chance of becoming broken links once the website hosting the magazine realized what they were hosting. Archive.org archives most things on the internet, and the link to the magazine was one of those things. The researcher had seen that Archive.org had been used previously by pro-ISIS groups on Twitter to ensure the links they send to each other are not broken. The researcher also noted that journalists and other anti-ISIS supporters appeared less likely to use archive.org as a url to show video or stills footage. Many journalists would use images or stills associated with their own news agency, and many anti-ISIS supporters were more likely to use these images rather than using ones likely to be pulled down by a social media site. By filtering the results of the Search API to only include urls that link back to Archive.org, the researcher was able to remove many false positives and focus the data set more on actual ISIS supporters.

The import results from the Search API resulted in 361 vertices (nodes) with 287 unique edges (relationships), 193 edges with duplicates (meaning the vertices tweeted along the same path), and a total of 480 edges. There were also 104 self-loops.

In-Degree. The top 20 users with the highest In-Degree Centrality were chosen for representation. These are the users that tweeted the most information out to other people.

Table 13

Highest In-Degree Centrality Amongst Twitter Search API Results for Critical Incident 3

User	In-Degree
shoutussalam	60
i_s_k_i	15
abunaseeha3	13
negarals	11
h_o_y_u	10
abo_talha23	9
milksheikhiraqi	8
states_mujahid2	8
wor_fn	7
myaccountis5	6
almusnet	6
hasyimabdullah4	6
isis_gun4	5
s	4
binjooher2	4
janeikelboom	4
greatisnation	4
islam4ea	3
xcfdre_87653	3
ejmalrai	3
sajen_24	3

Out-Degree. The top 20 users with the highest Out-Degree Centrality were chosen for representation. These are the users that received the most tweets from other users.

Table 14

Highest Out-Degree Centrality Amongst Twitter Search API Results for Critical Incident 3

User	Out-Degree
chyukaryori1	9
negarals	3
wildanzuhdi	3
mfadhly09	3
muslim_activist	3
hasyimabdullah4	2
islam4ea	2
muslimnewsurlph	2
emypriness	2
bintmath	2
iloveallah07	2
rezza_001	2
kucengireng	2
meidyayuda	2
jazrawi_camels	2
nina_noor9	2
sulaiman_dd	2
msaizul	2
hlavoix	2
dawlatulbaqiya	2
ssnn360	2

Betweenness Centrality. The top 20 users with the highest Betweenness Centrality Score were chosen for representation. These are the users that acted most as gatekeepers and bridges for the information. The higher their betweenness score, the more data that passes through them.

Table 15

Highest Betweenness Centrality Amongst Twitter Search API Results for Critical Incident 3

User	Betweenness Centraliy Score
shoutussalam	17787.667
chyukaryori1	15611.000
myaccountis5	12438.000
meidyayuda	12008.000
i_s_k_i	4798.000
abunaseeha3	4787.000
milksheikhiraqi	3542.000
h_o_y_u	3274.000
states_mujahid2	2406.000
negarals	2022.333
almusnet	1221.000
bintmath	1214.000
jazrawi_camels	1208.000
isis_gun4	918.000
nina_noor9	745.000
sulaiman_dd	745.000
hasyimabdullah4	617.000
abuhamza2365	614.000
msaizul	612.000
beb_911	612.000
s	308.667

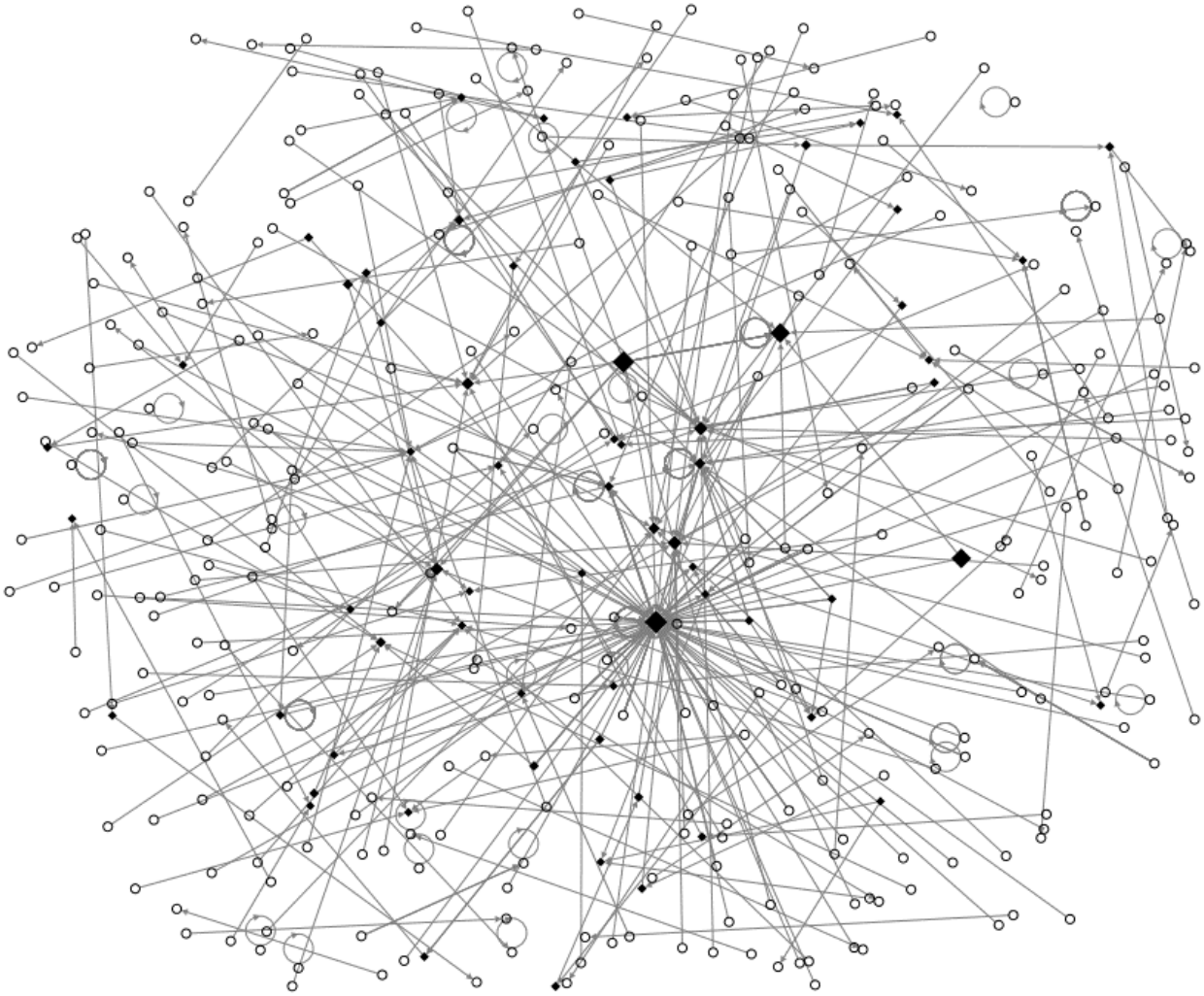


Figure 4. Visualization of the betweenness centrality scores for Critical Incident 3 using the Twitter Search API. This figure illustrates the highest betweenness centrality scores amongst the data.

Closeness Centrality. Closeness centrality is not a metric that can accurately be depicted simply by showing the top 20 users with the lowest metric score. All of the top 20 would have a closeness centrality score of 0 because it was a tweet from the user to nobody else. It was not a mention or reply to, so there is no other vertex for which the originating vertex to be close. The best way to show closeness centrality is to show the overall metrics for the network.

Table 16

Overall Scores for Closeness Centrality for Critical Incident 3 From the Twitter Search API

Metric	Result
Minimum Closeness Centrality	0.000
Maximum Closeness Centrality	1.000
Average Closeness Centrality	0.321
Median Closeness Centrality	0.059

Results for Critical Incident 3, Search API. The results from this Critical Incident closely resemble the results from Critical Incident 1, Search API. The user with the highest betweenness score (Table 15) correlates with the user with the highest in-degree score (Table 13). However, the high betweenness scores also include users that had high out-degree scores (Table 14). Again, like Critical Incident 1, Search API, the user who tweets the most to other people is the one who is the most like a gatekeeper of information within the network structure.

A striking difference between Critical Incident 3, Search API and Critical Incident 1, Search API is the closeness of the network. Critical Incident 1, Search API had an extremely close network with an average closeness centrality score of .024 (Table 8). Critical Incident 3, Search API, has a much higher closeness score with the average closeness centrality being .321 (Table 16). This means the overall network for this critical incident is not as close together as the other network patterns.

Figure 4 depicts the network graph with the solid diamonds representing high betweenness scores. The higher score, the bigger the solid diamond is. One can see that the user with the highest betweenness score (shoutussalam) is the main hub for information with smaller betweenness scores circling around him and then further away

from the main core larger betweenness scores start to appear as these users connect those in the middle to those more on the periphery.

The network pattern for Critical Incident 3, Search API shows a more back-and-forth flow of information between users. With both high in-degree and high out-degree users appearing in the high betweenness table (Table 15), the gatekeepers, and thus the central nodes of information, are both users that tweet out data and users that are simply mentioned in other tweets. This ebb and flow of information also expands out to more distant nodes as shown with the average closeness centrality score of .321. These results may differ from the other critical incidents because it offers "positive propaganda" as opposed to the violent imagery depicted in the other three. The magazine may attract more casual ISIS supporters than the violent imagery that likely appeals to a smaller, more hardcore group of militant supporters that were attracted to the immolation video (RAND, 2015).

DISCUSSION

The findings stated above will be used in this section to answer and support responses to the research questions mentioned at the beginning of the paper. All of the support questions will be answered with the hopes of identifying an answer for the overarching question of: How does ISIS's Twitter network affect the dissemination of its propaganda?

One of the main points affecting the configuration of the network will be the node or nodes of centrality. When all the measures of centrality are gathered together, they still point towards only one main node within the network. But, while there is still one "main" node in the network, it is not a centralized (sometimes referred to as a "wheel") network (Blum & Dudley, 2001), in which there is one main node that outputs information to all the other nodes. Nor is it a "Y" network in which there is one main node that then has branches to different points that end up forming a Y shape (Bokdia, 2008). Instead, the dissemination of ISIS propaganda on Twitter results in a node that is slightly more central than others, but then the network continues to produce other central nodes that connect to other users.

In addition to this, not all of these main nodes are necessarily outputting a large degree of information. As seen in Critical Incidence 1, Streaming API, the user that has the highest degree of betweenness centrality and who also appears at the center of the network in Figure 2 only tweeted once. It was the other users around this person that picked up the tweet and started sending the tweet to others while mentioning the author

of the original tweet. This means the originator of the tweet ended up in the center of the network because of the nodes around him, not because of his own continuous output. This did not remain the same in other networks. The other critical incidences showed either a correlation of betweeenness with in-degree score, or as the case in the bigger networks, a more even balance between in-degree, out-degree, and the overall betweenness score. This shows that the main nodes in the network were mostly facilitators of information by providing some information and then being used as an authority figure for others to output the information to other Twitter users. For the most part, the central users (nodes) were not simply figures who constantly tweeted out to others, but instead, were figures that acted as connectors to other users. This means that while each network had a more "central" node, they facilitated the conversation around them and were, in fact, supported by other nodes that continued the flow of information gained from the center. These other hubs were essential to continuing the spread of ISIS's propaganda, and in fact, result in the overall network structure of ISIS's Twitter network being a "scale-free network."

The discovery of the central hubs creates a scale-free network because the multiple nodes responsible for centrally disseminating ISIS information form what Barabasi and Bonabeau (2003) call hubs. These hubs are often part of the "scale-free network" (Barabasi & Bonabeau, 2003). A scale-free network follows a power law in that their degree distribution (the connectivity of their nodes) follows a power law (Li, Alderson, Doyle, & Willinger, 2006). These networks will have no natural number of edges (relationships between vertices), and instead can continue to grow as more and more nodes are added, thus they continue to scale in size. Barabasi and Albert (1999)

introduced the idea of scale-free networks in 1999 in reaction to the relationship they saw when studying the network structure of the World Wide Web. This structure occurs not only on the internet but also in nature, business, and other areas of study (Barabasi & Bonabeau, 2003). Different researchers have used different metrics and calculations to determine whether or not a network's degree distribution follows a power law (Mislove, Marcon, Gummadi, Druschel, Bhattacharjee, 2007; Ravid & Rafaeli, 2004; Wang & Chen, 2003.) For this research, the researcher found it best to use Ravid and Rafeli's (2004) method of using frequency versus degree in order to determine if the network followed a power law distribution. This method was chosen because it could use data already in NodeXL without having to use a more advanced social network analysis tool.

Power Law Distribution for Critical Incidents

Critical Incident 1, Streaming API. Figure 5 shows that the Distribution of the In-Degree for Critical Incident 1, Streaming API, follows a power law. This means that there are a lot of low in-degrees up front, but then it slowly evens out with a few high in-degree users at the tail end. Figure 6 for out-degree does not directly follow a power law because the users with high out-degree scores does not spike.

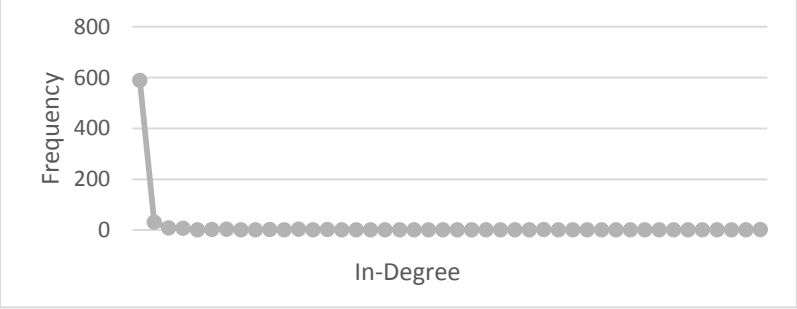


Figure 5. Plot chart showing In-Degree Distribution of Critical Incident 1, Streaming API. This chart illustrates the tail of In-Degree Distribution for Critical Incident 1, Streaming API.

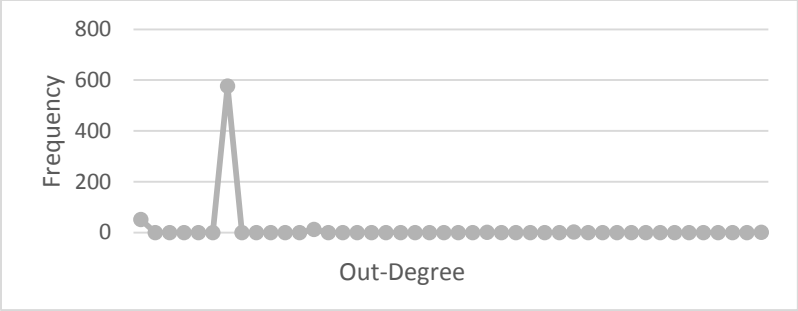


Figure 6. Plot chart showing Out-Degree Distribution of Critical Incident 1, Streaming API. This chart illustrates the lack of a curve of Out-Degree Distribution for Critical Incident 1, Search API.

Critical Incident 1, Search API. Figure 7 shows that the Distribution of the In-Degree for Critical Incident 1, Search API, follows a power law. This means that there are a lot of low in-degrees up front, but then it slowly evens out with a few high in-degree users at the tail end. Figure 8 for out-degree also follows a power law because the users with low out-degree are all up front, and then the few with high out-degree are at the end.

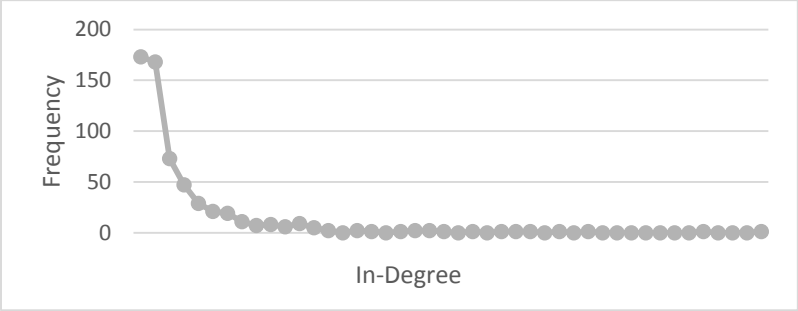


Figure 7. Plot chart showing In-Degree Distribution of Critical Incident 1, Search API. This chart illustrates the tail of In-Degree Distribution for Critical Incident 1, Search API.

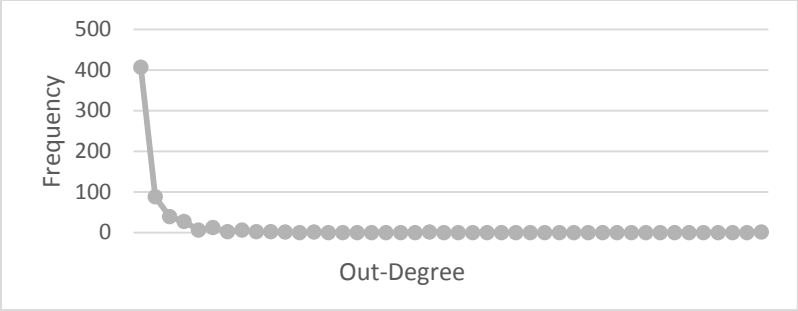


Figure 8. Plot chart showing Out-Degree Distribution of Critical Incident 1, Search API. This chart illustrates the tail of Out-Degree Distribution for Critical Incident 1, Search API.

Critical Incident 2, Streaming API. Critical Incident 2 had the lowest amount of user tweets in its results. This may have caused the differences in the graphs below. Figure 9 shows somewhat of a power law with a tail at the end that contains the users with a high score for in-degree and then the spike at the beginning of the graph for users that had low scores of in-degree. Figure 10 is an outlier from the rest of the network graphs. It shows a spike at the end of the graph which means there were a lot of users with a higher out-degree score. This may be explained by the fact that all the nodes in this network had an out-degree score of 0 or 1. This would explain the spike once the out-degree was equal to 1. The frequency then went up.

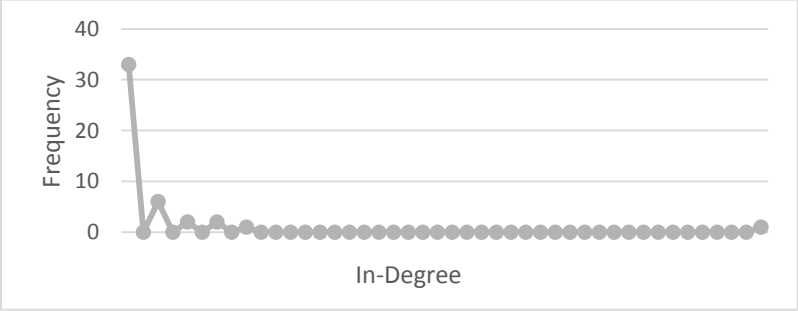
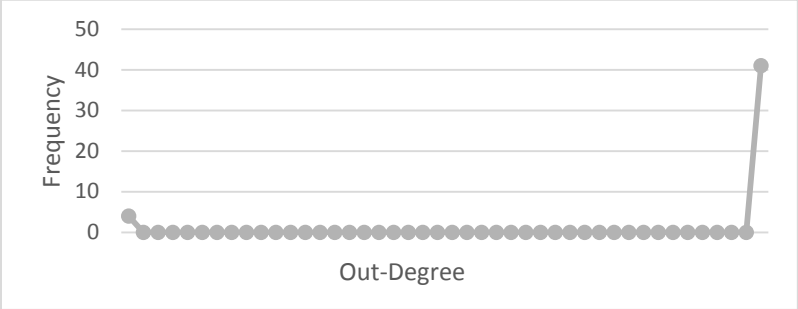


Figure 9. Plot chart showing In-Degree Distribution of Critical Incident 2, Streaming API. This chart illustrates the tail of In-Degree Distribution for Critical Incident 2, Streaming API.



.

Figure 10. Plot chart showing In-Degree Distribution of Critical Incident 2, Search API. This chart illustrates the In-Degree Distribution for Critical Incident 2, Search API.

Critical Incident 3, Search API. Figure 11 shows that the Distribution of the In-Degree for Critical Incident 3, Search API, follows a power law. This means that there are a lot of low in-degrees up front, but then it slowly evens out with a few high in-degree users at the tail end. Figure 12 for out-degree does not fit into the exact power law model because it spikes near the front instead of following more of a curve patter. This means that more users have a mid-range out-degree score than a low-score. There are a few users at the end who have higher out-degree scores.

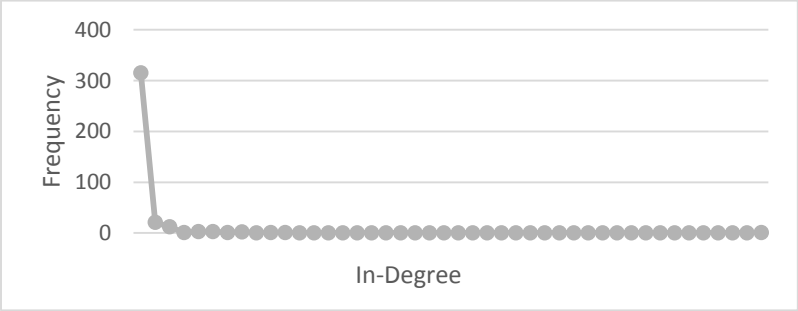


Figure 11. Plot chart showing In-Degree Distribution of Critical Incident 3, Search API. This chart illustrates the tail of In-Degree Distribution for Critical Incident 3, Search API.

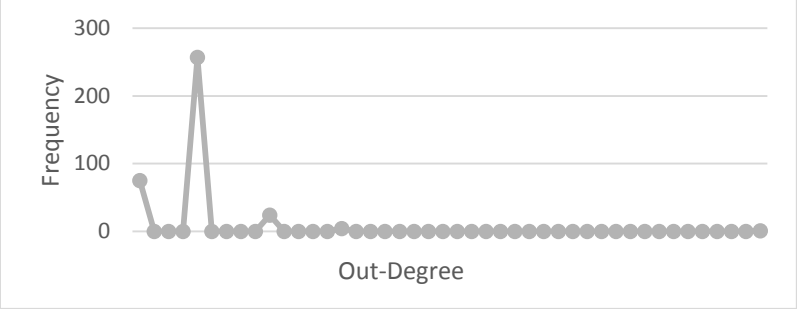


Figure 12. Plot chart showing Out-Degree Distribution of Critical Incident 3, Search API. This chart illustrates the spike of Out-Degree Distribution for Critical Incident 3, Search API.

Overall Results. The overall results from all of the critical incident networks seem to show that the larger network does have similarities with the scale-free network structure. Not every graph exactly followed this pattern, but most did, and the few that did not closely resemble the pattern had other factors affecting it (Figures 9 and 10 with such a low node count). The multiple nodes of centrality do, in fact, affect ISIS's overall network structure, and they cause the network structure to take on the properties of a scale-free network.

Since ISIS's Twitter network structure does have properties related to a scale-free network, this does affect the overall dissemination of its propaganda on Twitter. One of the main areas it affects is its ability to continue disseminating information even in the face of attack. One of the main qualities of a scale-free network is that it is resilient to random attacks (Barabasi & Bonabeau, 2003). Because of the many hubs of information in a scale-free network, several of the smaller ones can be taken out, either through

inherent failure or through attack, and the network as a whole will fill in the gap quickly and continue on. This resilience has been seen within the ISIS Twitter network already. On the same day ISIS released the video showing the beheading of hostage Kenji Goto, Twitter went on a widespread crackdown. This crackdown resulted in thousands of accounts being suspended. However, as the results to Critical Incident One in the Methodology section above show, ISIS supporters were quick to rebound and get back to spreading their propaganda. While the researcher was reviewing Twitter results on January 31st, 20015, ISIS supporters were boasting about being suspended and coming back so quickly in order to continue spreading information. Many users bragged about coming back from suspension and spread the beheading link all in the same tweet. The overall ISIS Twitter network is too resilient and robust to simply be taken down by random suspensions.

Another example of how the network affects dissemination is in its ability to grow and increase its output of propaganda on Twitter. The premise behind a scale-free network is that it can grow without destroying network communication (Hein, Schwind, & Konig, 2006). This growth is supported by the probability of new hubs connecting to older, more well-established hubs. Furthermore, this growth can occur in an evolutionary pattern, unlike random networks (also called ER networks) that start out with a fixed number of nodes (Hein et al., 2006). While studying the evolution of genes, Willeboordse (2006) noted that a scale-free network supports diversity and reproducibility, and that this helps to create an overall stronger network. These same two traits also hold true for a social media network in that the scale-free network makes it

easier for new nodes to connect to the network enhancing reproduction and diversity of the overall communication network.

For ISIS, the ability to grow and evolve all while resisting being taken down by an attack is exactly what their Twitter media plan is meant to do. ISIS has obviously made their media plan a top priority. By crafting their network – inherently or not – in such a way that it can easily grow while at the same time resist attacks and Twitter suspensions, ISIS continues to be a force on Twitter.

A scale-free network also supports the content of the spread of propaganda. Scale-free networks tend to be homogenous in thought and easily influenced by the main hubs. Hein et al. (2006) discovered this when they set up a simulation of a scale-free network of security traders. According to Hein et al. (2006), information about stocks spread "like an epidemic" through the scale-free network, but it was directly influenced by the opinion of the main hubs (p.273). Other agents would change their decision based on any and all changes instituted by the power hubs. This resulted in heavy fluctuation within the simulated market because once an opinion came from a power hub, the whole market would change its opinion. For ISIS, this means that it is not easy to express individual opinions and then have these opinions taken up by the overall network.

The particular implications of the scale-free network structure for ISIS are that it can resist attack, continue to easily grow and scale, maintain control of content, and it can continue to connect with users who are not necessarily current ISIS supporters. The central nodes in each hub act as gatekeepers for the information. This conversation between gatekeeper and other nodes allows for current supporters to gain information while also allowing more users to be brought into the fold. By allowing increased output

and enabling evolutionary growth (Willeboordse, 2006), ISIS's Twitter network can not only be effective at outputting information but also at continuing to grow the network. The whole point of ISIS's propaganda is to attract reaction, and by attracting reaction, to gain supporters. By easily allowing growth, resisting attacks, and maintaining overall content, the ISIS Twitter network is highly effective at spreading propaganda and thus growing its overall support networks.

CONCLUSION AND CONTRIBUTIONS

This study sought to answer the overall question of how ISIS's Twitter network configuration affects the dissemination of its propaganda. By focusing on the nodes of centrality, the role of these nodes in dissemination of information, and the overall network structure formed by these nodes, the researcher was able to come to the conclusion that this particular network (ISIS's propaganda network) forms a scale-free network. This scale-free network means that there are multiple hubs that each have one centralized node, and that these hubs are then connected to each other. This type of network is not a completely centralized network like a Wheel or a Y network, but instead, it is more decentralized and offers more affordances for the purpose of spreading propaganda. The affordances of this network to ISIS in their purpose of distributing propaganda are resilience, growth, and uniformity. The scale-free network allows the overall Twitter propaganda network to resist random attacks, continue to grow and add new users to older, well-maintained central hubs, and to ensure that the propaganda released and disseminated aligns with ISIS's overall ideology and media strategy. Understanding this overall network and its affordances is important because ISIS represents a more advanced threat on social media, and learning the ins and outs of this threat can help to come up with ways to fight it (Berger & Morgan, 2015). While the research in this paper is specific to ISIS, other terrorists groups will likely learn from ISIS's successful campaign and will start to place more attention on social media platforms. Learning ISIS's network can help provide a baseline for other terrorists

groups on social media, and it may eventually help with keeping these groups from disseminating their propaganda on these platforms. Knowledge of ISIS's Twitter network can help provide a key to stopping not only them but also others that are likely to follow in their path.

Implications for Practice

This study presents an overall view of ISIS's Twitter network. This view can be used in practice to help defeat ISIS on Twitter. The only true way to stop ISIS from spreading their propaganda across the Twitter network would be to prevent ISIS and their supporters from posting on Twitter at all. Unfortunately, this is highly unlikely to happen because ISIS supporters have shown how adept they are at getting around censorship. Another option would be to use the Achilles' Heel of the scale-free network. While a scale-free network is resilient to random attacks, its "Achilles' Heel" (Barabasi &Bonabeau, 2003) is its inability to withstand a targeted attack. When the attack is random, it is likely that only the smaller hubs will be taken out, and these smaller hubs are easily replaced. But, if a targeted attack hits the main hubs, this makes it harder for the network to bounce back. For ISIS, as long as Twitter just keeps suspending random followers, their network will be okay and will continue in its ability to grow and evolve. Right now, Twitter has suspended at least 1,000 accounts between September and December of last year (Gladstone & Goel, 2015), and probably another 2,000 or more in the last few weeks (Ross, Meek, & Ferran, 2015), but these suspensions have done little to slow down the overall network. Twitter is likely just shutting down accounts that show support for ISIS without identifying how connected these accounts are to other accounts. If Twitter or other intelligence agencies with the capability to study such large

data sets could pinpoint some of the hubs of the ISIS Twitter network, and then all at once take down those central hubs, it would make it harder for ISIS to come back as quickly as they have done before. Repeatedly removing the central hubs of the network *should* slow down how quickly they can disseminate their propaganda.

Another implication of the network structure that could be used to eventually stop ISIS on Twitter is the ability to use misdirection. Since the scale-free network is dependent upon the opinions of the few hubs, if the opinion of those power hubs changes, then the overall network could possibly change as well. This would obviously require a lot of work behind the scenes from government agencies, but it is a tactic that has proven to work in the past for physical warfare and is coming to the rise in cyber warfare (Breuer, 2002; Carr, 2011). Misdirection, the art of disguising true intentions in order to gain an advantage, has been used for centuries with some of the biggest examples coming in World War II with the misdirection projects used by the Allies to make the Luftwaffe waste many bombs on empty fields (Breuer, 2002). The most anecdotal example of misdirection is the Trojan Horse; manipulate people into thinking one thing in order to gain entry and complete the initiative. Misdirection is also being used by cyber criminals (ThreatMetrix.com, 2013) and even, supposedly, by countries such as the Russian Federation (Carr, 2011). If the power hubs of ISIS supporters were manipulated into tweeting out something that may not necessarily support – or help strengthen – the overall network, then that opinion would begin to spread throughout the whole network, and this could possibly make changes to the overall opinion and ideology of the network. While this type of cyber misdirection against a terrorist organization has not been done (openly, at least), it would attack the scale-free network at one of its weak points.

Limitations

There were limitations to what data the researcher was able to collect. As mentioned above, the Twitter APIs only collect a certain amount data, so the researcher was unable to acquire 100% of all tweets matching a specific keyword. The research could also only match keywords that were English because of the lack of knowledge about the Arabic language. This presented a special limitation because many tweets would have the keyword in English but the rest of the tweet text would be in Arabic. These tweets were considered because the keyword or hashtag itself was in English and was readable by the researcher. Due to this, only the keyword or hashtag was considered when collecting data. There may have been more propaganda information in the rest of the tweet, but only the English keywords and hashtags mattered.

Time was also a limiting factor. The Python script did not automatically start itself when an incident occurred. The researcher had to ascertain what keywords would be most worthwhile to use, input them into the script, and then set the script running. Because of this, there is no certainty that the beginning node of the tweets was collected in the information. While the Twitter Search API used by NodeXL had the capabilities to pick up past tweets to complement the tweet gathered from the Streaming data, there is no guarantee that all of the first tweets were gathered, or even that all tweets in general were gathered. Likewise, if three-fourths of ISIS's followers and supporters were using one keyword or hashtag, and the researcher chose to use the keyword or hashtag that the other one-fourth of the followers and supporters were using, then not all tweets relevant to the critical incidents were gathered.

Another limitation to the collection of data is the nature of the tweets and users themselves. ISIS is not a capitalist corporation or a non-profit, it is an organization classified as a terrorist group by the United Nations (UN.org, 2015), the European Union (Wahlisch, 2010), and many other world powers. Their presence and the information they disseminate are often restricted. Many of ISIS's followers and supporters have their accounts suspended and their information deleted. This became even more relevant after ISIS released the first video of Japanese hostage Kenji Goto (Shiloach, 2015). Between that time and the later release of Goto's execution video, Twitter suspended more than 1,400 ISIS accounts, many shortly after the release of the execution video. These suspensions have not stopped. The last week of February 2015 saw more than 2,000 ISIS accounts suspended (Ross, Meek, & Ferran, 2015). Many of these suspended and deleted accounts were rich data sources for the hashtags and keywords necessary for data collection. There is no way to get them back. Due to suspended and deleted accounts, there will not be 100% relevant and complete data collected.

Two other limitations of this research are focused on bias and reliability. The bias comes from the researcher. As a Western-born and educated non-Muslim, the researcher is an outsider to most of these communities. And, while this outside perspective can help in being a neutral, non-biased researcher, it also means that there are aspects of the culture and ideology that the researcher will not understand and may be unable to truly comprehend. This is mostly seen with the limitation on language. Lack of Arabic language skills means that the researcher is assuming that if the Tweet includes the English keywords, then it is relevant. This relevancy also plays into the reliability because there was no way for the researcher to verify if the Twitter user was who they

said they were or even if they believe what they said they believe in. The researcher does not have the contacts nor the resources to look into verifying such information. If the user had tweets supporting ISIS, images supporting ISIS, and claimed to be an ISIS supporter, then the researcher assumed they were an ISIS supporter. All of the above information may have biased or limited the collected data and may have influenced the results.

APPENDIX

The following narrative will take the reader through how the researcher decided whether to use the Search API, Streaming API, or both and what hashtags to use when deciding how to gather data. This narrative will focus on Critical Incident 3, the release of *Dabiq* magazine. On February 12th, the research became aware that ISIS had realized another propaganda magazine. Knowing this would be a big event for ISIS supporters, the research started looking at ISIS supporters on Twitter, many, if not all, of whom are now suspended and whose accounts have been deleted. By looking through these accounts, the researcher realized that unlike the execution videos – which almost always used the title of the video to trend a hashtag – there was no seemingly discernable English-language hashtag to use. Because of this lack of discernable hashtag, the researcher decided against using the Streaming API because it would result in too many false positive results for the researcher to manually analyze. Instead, the researcher decided to use NodeXL's import from Twitter function because it would gather and format data into an easier-to-use format than the Streaming API. In order to see what hashtag should be used, the researcher started inserting search keywords into the import from Twitter search function to see what kind of information appeared. After reviewing the ISIS supporters on Twitter, the researcher decided to simply "Dabiq" to gather data and to see if there would be any way to filter the data in order to gain the most relevant data set for analysis. The brief results that came up from this search term also included the url from which the magazine was linked. The researcher noticed that archive.org was

a frequent url in the results list. Knowing from previous research and use of Twitter, the researcher knew that archive.org was often used by ISIS supporters to tweet links to images or videos that they wanted to ensure would not be broken by being removed by the overarching host. The researcher chose a handful of tweets that contained an archive.org url to review, and the tweets either contained pro-ISIS sentiment or the users themselves had a Twitter that name that showed support for ISIS. Based on this, the researcher decided to filter this small result set and then review the data. Once filtered, the data showed a lot of ISIS supporters that were interconnected. This graph of the small data set convinced the researcher to use the keyword "Dabiq" and then to filter the final results in order to gain the most relevant data. Twenty-four hours after the initial release of the magazine, the researcher went back and entered the keyword "Dabiq" into the import from Twitter search feature. The results of this search were then filtered for the archive.org url, reviewed to ensure that the collected data still contained relevant results, and then finally, this data set was used for final review for Critical Incident 3.

BIBLIOGRAPHY

Altman, Alex. (2014). Why terrorists love Twitter. *TIME*. Retrieved from http://time.com/3319278/isis-isil-twitter/

Anderson, John. (2006). Qualitative and quantitative research. Retrieved from https://www.icoe.org/webfm_send/1936

Anti-Defamation League. Hashtag terror: How ISIS manipulates social media. Retrieved from http://www.adl.org/combating-hate/international-extremism-terrorism/c/isis-islamic-state-social-media.html

Archetti, C. (2012). *Understanding terrorism in the age of global media*. USA: Palgrave Macmillan.

Barabasi, A. (2009). Scale-free networks: A decade and beyond. *Science*, 325, p.412-413.

Barabasi, A. & Bonabeau, E. (2003). Scale-free networks. *Scientific American*, 288, p.60-69.

Barrat, A., Barthelemy, M., Pastro-Satorras, R., & Vespignani, A. (2004). The architecture of complex weighted networks. *PNAS*, 101(11), p.3747-3752.

BBC News. (2015, February 1). Japan outraged at IS 'beheading' of hostage Kenji Goto. *BBC News*. Retrieved from http://www.bbc.com/news/world-middle-east-31075769

BBC News. (2015, February 3). Jordan pilot hostage Moaz al-Kasasbeh 'burned alive.' *BBC News*. Retrieved from http://www.bbc.com/news/world-middle-east-31121160

Berger, J. M. (2014). How ISIS games Twitter. *The Atlantic*. Retrieved from http://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/

Berger, J.M. (2015, March 13). Taming ISIS on Twitter: More than a game of whack-a-mole. *CNN*. Retrieved from http://www.cnn.com/2015/03/13/opinions/isis-twitter-crackdown/

Bowen, Glenn. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), pages 27-40.

Broder, Jonathan. (2015, February 11). Jordan goes all in against ISIS, but for how long? *Newsweek*. Retrieved from http://www.newsweek.com/2015/02/27/jordan-goes-all-against-isis-how-long-306093.html

Breuer, W., (2002). *Deceptions of World War II*. USA: John Wiley & Sons.

Bruggeman, Jeroen. (2013). *Social networks: An introduction*. USA: Routledge.

Caldarelli, G. (2007). *Scale-free networks: Complex webs in nature and technology*. Oxford: Oxford University Press.

Carr, J. (2011). *Inside cyber warfare: Mapping the cyber underworld*. USA: O'Reilly Media Inc.

Center for Middle East Policies at Brookings Institute. (2015). *The ISIS Twitter census: Defining and describing the population of ISIS supporters on Twitter*. Washington, D.C.: J.M. Berger & J. Morgan.

CNN Library. (2014). ISIS fast facts. *CNN.com*. Retrieved from http://www.cnn.com/2014/08/08/world/isis-fast-facts/

CNN Wire. (2014). ISIS, ISIL, or the Islamic State? *CNN.com*. Retrieved from http://go.galegroup.com/ps/i.do?id=GALE%7CA381987011&v=2.1&u=unc_main&it=r&p=STND&sw=w&asid=2ebd27af5c3eb2a3174456f614b7e5fc

Conway, Maura. (2006). Terrorism and the Internet: New media – new threat? *UK Politics and the Internet – The first decade*, 59(2).

D'Souza, Steven. (2015, March 6). ISIS supporters on Twitter come from small group, study says. *CBC News*. Retrieved from http://www.cbc.ca/news/world/isis-supporters-on-twitter-come-from-small-group-study-says-1.2984733

Denning, Dorothy. (2009). Terror's web: How the internet is transforming terrorism. In Y. Jewkes and M. Yar (eds.), *Handbook on Internet Crime*. Willan Publishing.

Department of the Army. (2014). Insurgencies and countering insurgencies (Publication FM 3-24/MCWP 3-33.5, C1). Washington, D.C.: Department of the Army.

Doyle, J., Alderson, D., Li, L., Low, S., Roughan, M., Shalunov, S., Tanaka, R., & Willinger, W. (2005). The "robust yet fragile" nature of the internet. *PNAS*, 102(41), 14497-14502.

Druckman, J., Kifer, M., & Parkin, M. (2014). U.S. congressional campaign communications in an internet age. *Journal of Elections, Public Opinion, and Parties*, 24(1), p.20-44.

Fleming, L., King, C., & Juda, A. (2007). Small worlds and regional innovation. *Organization Science*, 18(6), 938-954.

Frand, Jason. (n.d.). Data mining: What is data mining? Retrieved from http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm

Gladstone, R. & Goel, V. (2015, March 5). ISIS is adept on Twitter, study finds. *NY Times*. Retrieved from http://www.nytimes.com/2015/03/06/world/middleeast/isis-is-skilled-on-twitter-using-thousands-of-accounts-study-says.html?_r=0

Glint, M. (2014). *Can a war with ISIS be won?* USA: Conceptual Kings.

Gyarmati, L. & Trinh, T. (2010). Scafida: A scale-free network inspired data center architecture. *ACM SIGCOMM computer communication review*, 40(5), p.5-12.

Hall, B. (2015). *Inside ISIS: The brutal rise of a terrorist army*. USA: Center Street.

Han, J., Kamber, M., & Pei, J. (2011). *Data mining: Concepts and techniques*. Waltham, MA: Elsevier Inc.

Hansen, D., Shneiderman, B., & Smith, M. (2010). *Analyzing social media networks with NodeXL: Insights from a connected world*. USA: Morgan Kaufmann.

Hein, O., Schwind, M., & Konig, W. (2006). Scale-free networks: The impact of fat tailed degree distribution on diffusion and communication processes. *Wirtschaftinformatik*, 48(4), p.267-275.

Irshaid, Faisal. (2014). How ISIS is spreading its message online. *BBC News*. Retrieved from http://www.bbc.com/news/world-middle-east-27912569

Jick, Todd. (1979). Mixing qualitative and quantitative methods: triangulation in action. *Administrative Science Quarterly*, 24(4), page 602-611.

Katz, Rita. (2014). Follow ISIS on Twitter: A special reports on the use of social media by jihadists. *Insite Blog on Terrorism & Extremism*. Retrieved from http://news.siteintelgroup.com/blog/index.php/entry/192-follow-isis-on-twitter-a-special-report-on-the-use-of-social-media-by-jihadists

Kingsley, P. (2014, June 23). Who is behind ISIS's terrifying online propaganda operation? *The Guardian*. Retrieved from http://www.theguardian.com/world/2014/jun/23/who-behind-isis-propaganda-operation-iraq

Johnson, R. & Christensen, L. (2013). *Educational research: Quantitative, qualitative, and mixed approaches*. US: Sage Publications.

Jowett, G. & O'Donnell, V. (2006). *Propaganda and persuasion*. USA: Sage.

Kaplan, A. & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, 53(1), p.59-68.

Kjujka, Deana. (2013). When terrorists take to social media. *The Atlantic*. Retrieved from http://www.theatlantic.com/international/archive/2013/02/when-terrorists-take-to-social-media/273321/?single_page=true

Knoke, D. (2008). *Social network analysis*. USA: Sage.

Lancichinetti, A., Radicchi, F., Ramasco, J., & Fortunato, S. (2011). Finding statistically significant communities in networks. *PLos ONE*, 6(4), pages 1-18.

Li, L., Alderson, D., Doyle, J., & Willinger, W. (2006). Towards a theory of scale-free graphs: Definition, properties, and implications. *Internet Mathematics*, 2(4), p.431-523.

Mislove, A., Marcon, M., Gummadi, K., Druschel, P., & Bhattacharjee, B. (2007). *Proceedings from the IMC'07*: Measurement and analysis of online social networks. CA: San Diego.

Newman, M. (2003). A measure of betweenness centrality based on random walks. *Social Networks*, 27(1), p.39-54.

Nissen, Thomas. (2014). Terror.com – IS's social media warfare in Syria and Iraq. *Military Studies Magazines: Contemporary Conflicts*, 2(2), pages 1-8.

Neuman, Scott. (2015, January 31). Video appears to show beheading of Japanese hostage Kenji Goto. *NPR*. Retrieved from http://www.npr.org/blogs/thetwo-way/2015/01/31/382902139/video-purports-to-show-beheading-of-japanese-hostage-kenji-goto

O'Callaghan, D., Prucha, N., Greene, D., Conway, M., Carthy, J., & Cunningham, P. (2014). Online social media in Syria conflict: Encompassing the extremes and the in-betweens. From the Proc. 2014 *International Conference on Advances in Social Network Analysis and Mining* (ASONAM 2014)

Okamoto, K., Chen, W., & Li, X. (2008). Ranking of closeness centrality for large-scale social networks. *Frontiers in Algorithmics*, 5059, p.186-195.

Olsen, Wendy. (2004). Triangulation in social research: Qualitative and quantitative methods can really be mixed. In M. Holborn Editor, *Developments in Sociology*. Ormskirk: Causeway Press.

Opsahl, Tore. (2010). Node centrality in weighted networks: Generalizing degree and shortest paths. *Social Networks*, 32(3), p.245-251).

Providence Research. (2014). *The ISIS threat: The rise of the Islamic State and their dangerous potential*. USA: Providence Research.

Rabil, Robert. (2014). The ISIS chronicles: A history. *The National Interest*. Retrieved from http://nationalinterest.org/feature/the-isis-chronicles-history-10895?page=2

Rampe, D. (2013, February 26). Magic is misdirection. *ThreatMetrix*. Retrieved from http://www.threatmetrix.com/magic-is-misdirection-often-so-is-cybercrime-ddos-attack-helps-cyberthieves-make-900k-disappear-from-company-bank-account/

Ravid, G. & Rafaeli, S. (2004). Asynchronous discussion groups as Small World and Scale Free networks. *First Monday*, 9(6).

Ressler, Steve. (2006). Social Network Analysis as an approach to combat terrorism: Past, present, and future research. *Homeland security affairs*, II(2), pages 1-10

Rodrigue, Jean-Paul. (2015). The geography of transport systems. Retrieved from https://people.hofstra.edu/geotrans/eng/ch1en/conc1en/networkstructure.html

Ross, B., Meek, J., & Ferran, L. (2015, March 2). Twitter escalates its own ISIS battle: 2,000 accounts suspended last week. *ABC News*. Retrieved from http://abcnews.go.com/International/twitter-escalates-isis-skirmish-2000-accounts-suspended-week/story?id=29335434

Ryan, Laura. (2014). Al-Qaida and ISIS use Twitter differently. Here's how and why. *The National Interest*. Retrieved from http://www.nationaljournal.com/tech/al-qaida-and-isis-use-twitter-differently-here-s-how-and-why-20141009

Ryan, M. (2014). Hot issue: Dabiq: What Islamic State's new magazine tells us about their strategic direction, recruitment patterns and guerrilla doctrine. *The Jamestown Foundation*. Retrieved from http://www.jamestown.org/single/?tx_ttnews[tt_news]=42702&no_cache=1#.VRqo1eGOWPZ

Scott, J. (2012). *Social network analysis*. USA: Sage.

Seib, P. & Janbek, D. (2010). *Global terrorism and new media: The post Al Qaeda generation*. USA: Routledge.

Shane, Scotty & Hubbard, Ben. (2014). ISIS displaying a deft command of varied media. *The New York Times*.

Sheridan, P., Kamimura, T., & Shimodaira, H. (2010). A scale-free structure prior for graphical models with applications in functional genomics. *PLos One*, 5(11).

Shiloach, Gilad. (2015, February 3). ISIS is hijacking western Twitter accounts to rebuild terror network. *Vocativ*. Retrieved from http://www.vocativ.com/world/isis-2/isis-twitter-accounts/

Shirky, Clay. (2011). The political power of social media: Technology, the public sphere, and political change. Council on Foreign Relations.

Speri, Alice. (2014). ISIS fighters and their friends are total social media pros. *Vice News*. Retrieved from https://news.vice.com/article/isis-fighters-and-their-friends-are-total-social-media-pros

Stemler, Steve. (2001). An overview of content analysis. *Practical Assessment, Research & Evaluation*, 7(17). Retrieved December 6, 2014 from http://PAREonline.net/getvn.asp?v=7&n=17

Stern, J. & Berger, J. M. (2015). *ISIS: The state of Terror*. USA: Harper Collins.

Stone, Jon. (2014). Islamist fighters in Irag and Syria keep tweeting pictures of their cats. *Buzzfeed*. Retrieved from http://www.buzzfeed.com/jonstone/foreign-jihadi-fighters-in-iraq-and-syria-keep-tweeting-pict

Stone, J. (2014, August 22). Blocked on Twitter and YouTube, ISIS turns to Diaspora and VKontakte to disseminate message. *IB Times*. Retrieved from http://www.ibtimes.com/blocked-twitter-youtube-isis-turns-diaspora-vkontakte-disseminate-message-1666758

The Clarion Project. (2014, September 10). The Islamic State's (ISIS, ISIL) Magazine. *The Clarion Project*. Retrieved from http://www.clarionproject.org/news/islamic-state-isis-isil-propaganda-magazine-dabiq

Tyler, J., Wilkinson, D., & Huberman, B. (2003). Email as spectroscopy: Automated discovery of community structure within organizations. In M.H. Huysman, E. Wenger, & V. Wulf (Eds.), *Communities and Technologies* (81-96). Netherlands: Springer.

United States Institute of Peace. (2004). How modern terrorism uses the Internet. Washington, D.C.: Gabriel Weimann.

United States Institute of Peace. (2014). Syria's socially mediated civil war. Washington, D.C.: Lynch, M., Freelon, D., & Aday, S.

Van Praagh, Peter. (2014). Statement by the President of the Halifax International Security Forum on ISIL's propaganda video and the use of the #HISF2014. *Halifax the Forum*. Retrieved from http://halifaxtheforum.org/news/statement-by-the-president-of-the-halifax-international-security-forum-on-isils-propaganda-video-and-the-use-of-the-hisf2014

Walker, L. (2015, March 6). Inside the ISIS social media campaign. Newsweek. Retrieved from http://www.newsweek.com/inside-isis-social-media-campaign-312062

Wang, X. & Chen, G. (2003). Complex networks: Small-world, scale-free and beyond. *IEEE circuits and systems magazine*.

Weimann, Gabriel. (2011). Al Qaeda has sent you a friend request: terrorists using online social networking. Israeli Communication Association.

Weimann, Gabriel. (2014a). New terrorism and new media. Commons Lab of the Woodrow Wilson International Center for Scholars, Washington, DC.

Weimann, Gabriel. (2014b). Social media's appeal to terrorists. *Insite Blog on Terrorism & Extremism*. Retrieved from

http://news.siteintelgroup.com/blog/index.php/entry/295-social-media%E2%80%99s-appeal-to-terrorists

Weiss, M. & Hassan, H. (2015). *ISIS: Inside the army of terror*. USA: Simon and Schuster.

Wiener-Bronner, Danielle. (2014). Twitter is the preferred social media platform among terrorists. *The Wire*. Retrieved from http://www.thewire.com/global/2014/05/social-media-terrorism-rises/370893/

Willeboordse, F. (2006). Dynamical advantages of scale-free networks. *Physical Review Letters*, 96.

Xu, G., Zhang, Y., & Li, L. (2010). Web mining and social networking: techniques and applications. US: Springer Publishing.

Yang, C. & Ng, Tobun. (2007). Terrorism and crime related weblog social network: Link, content analysis and information visualization. From the Intelligence and Security Informatics Session, 2007 *IEEE Conference*.

Zayadin, H. (2015, March 5). Fighting words: Inside the social media war against ISIS. *PBS*. Retrieved from http://www.pbs.org/mediashift/2015/03/fighting-words-inside-the-social-media-war-against-isis/

Zelin, Aaron. (2013). The state of global jihad online. *New America Foundation*.